The New EU Data Protection Regime: Setting Global Standards for The Right to Personal Data Protection.

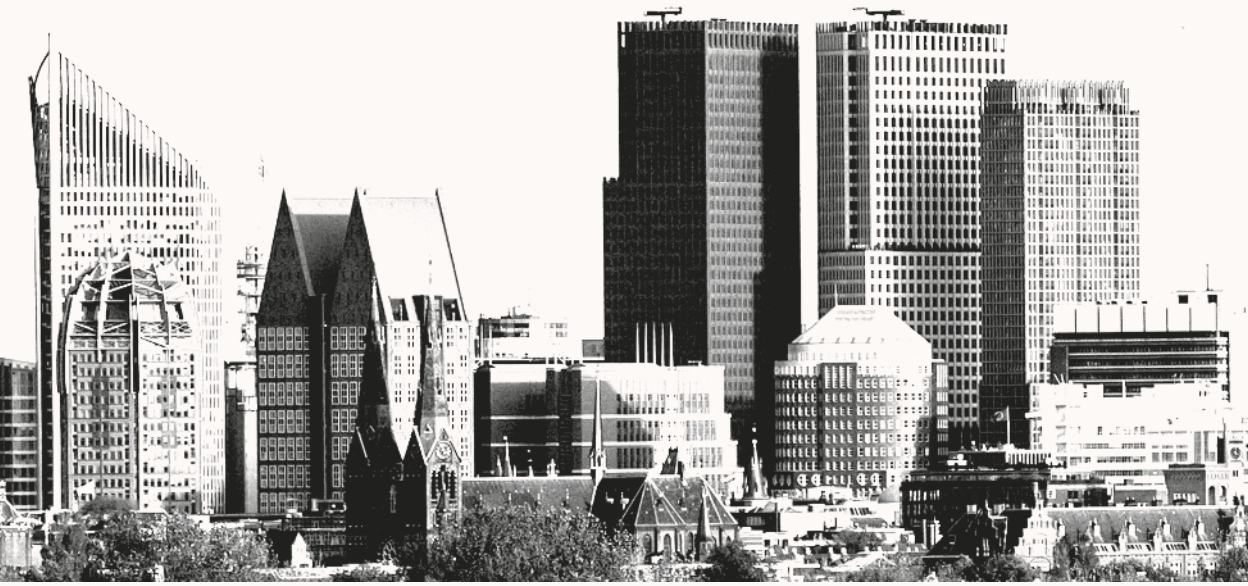
Rijpma, J.J.

FIDE XXIX Congress The Hague 2020

THE NEW EU DATA PROTECTION REGIME: SETTING GLOBAL STANDARDS FOR THE RIGHT TO PERSONAL DATA PROTECTION

THE XXIX FIDE CONGRESS IN THE HAGUE
2020 CONGRESS PUBLICATIONS

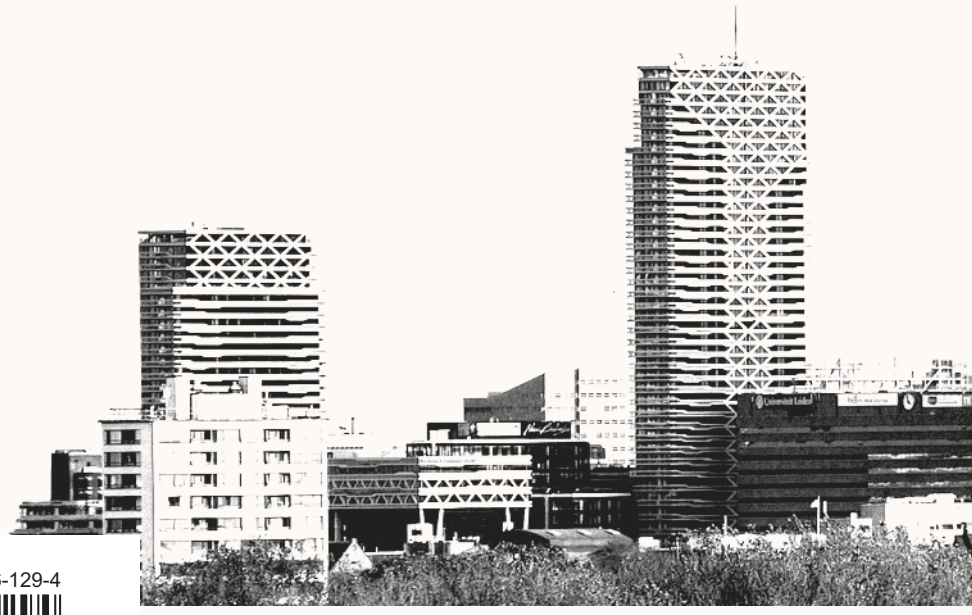
VOL. **2**



Jorrit J. Rijpma (Ed.)

eleven
international publishing

The proceedings of the XXIX FIDE Congress in The Hague in 2020 are published in four volumes. This book (Vol. 2) contains the reports of the General Rapporteur (Orla Lynskey), the Institutional Rapporteurs (Herke Kranenborg and Anna Buchta) and the National Rapporteurs on Topic 2: The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection.



ISBN 978-94-6236-129-4

FIDE XXIX Congress The Hague 2020

The New EU Data Protection Regime

The New EU Data Protection Regime

Setting Global Standards for the Right to Personal Data Protection

Le nouveau cadre reglementaire de l'UE en matiere de protection des donnees

L'enonciation de normes mondiales pour le droit a la protection des donnees personnelles

Das neue EU Datenschutzregime

Setzen globaler Standards für das individuelle Recht auf Datenschutz

The XXIX Congress in The Hague, 2020
Congress Publications Vol. 2
Editor: Jorrit J. Rijpma
General Rapporteur: Orla Lynskey
Institutional Rapporteurs: Anna Buchta & Herke Kranenborg

eleven
international publishing

Published, sold and distributed by Eleven International Publishing
P.O. Box 85576
2508 CG The Hague
The Netherlands
Tel.: +31 70 33 070 33
Fax: +31 70 33 070 30
e-mail: sales@elevenpub.nl
www.elevenpub.com

Sold and distributed in USA and Canada
Independent Publishers Group
814 N. Franklin Street
Chicago, IL 60610
USA
Order Placement: (800) 888-4741
Fax: (312) 337-5985
orders@ipgbook.com
www.ipgbook.com

Eleven International Publishing is an imprint of Boom uitgevers Den Haag.

ISBN 978-94-6236-129-4

Printed in the Netherlands

Table of Contents

Introduction from the FIDE 2020 Board

It was in a small pub in Tallinn in 2012, late at night, that a group of Dutch jurists visiting the bi-annual Congress of the International Federation for European Law (FIDE) in Estonia, brought up the bold idea of bringing FIDE to The Netherlands. Eight years later, the Netherlands Association of European Law (NVER), has the honour of welcoming the members of FIDE in The Hague at the XXIX FIDE Congress. Or rather: welcoming them back to The Hague. Twice before did the FIDE convene in the Dutch seat of government: in 1963 and in 1984. Much like the European Union itself, The Hague has changed since 1984. It has grown, its skyline has been transformed and its position as an international city of peace and justice consolidated, also with the presence of Europol and Eurojust.

The impact of FIDE as an organisation, and of its members, on the development of European law has been well-documented.[1] From the outset FIDE formed a unique transnational network bringing together key actors who stood at the basis of the 'new legal order',[2] who shaped European law as a discipline in its own right, and who legitimised the Court's "'constitutional' understanding of European Law" at its early conferences in The Hague (1963) and Paris (1965).[3]

Whereas in the early 1960s European law had yet to achieve its full potential, participants of the 1984 Congress may have considered primacy and direct effect as largely settled, as the European Communities were to embark on Jacques Delors' internal market project. At the same time, they would not have imagined the exponential growth in services and the exciting, yet also disruptive, effects of the internet and new technology. In 2020, after years of crises that have shaken the European Union to its very foundations, it seems once again in need of FIDE to act as "the wheeling flank of the army of European jurists",[4] to understand, explain and defend a Union that is based on the rule of law and, notably, on

1 J. Laffranque, 'FIDE – Uniting Great Minds of European Law: 50 Years of the International Federation for European Law', Juridica International XVIII, 2011, pp. 173-181. See for example also S. Lee Mudge & A. Vauchez, 'Building Europe on a Weak Field: Law, Economics, and Scholarly Avatars in Transnational Politics' AJS Vol. 118, No. 2, 2012, pp. 449-492. The Spanish FIDE 2010 organisation did a fantastic job in making much of the FIDE archive accessible to its members: www.fide-europe.org/members-login/, visited 1 February 2020.

2 Judgment of 5 February 1963, Case 26/62, NV Algemene Transport-en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, ECLI:EU:C:1963:1.

3 M. Rasmussen, Establishing a Constitutional Practice of European Law: The History of the Legal Service of The European Executive, 1952-65, Contemporary European History Vol. 21, No. 3, 2012, p. 395.

4 A. de Vreese, Droit communautaire et droit national, 14 Cahiers de Bruges, Vol. 14, No. 399, 1965, quoted in A. Vauchez, Brokering Europe: Euro-Lawyers and the Making of a Transnational Polity, Cambridge, Cambridge University Press, 2015, p. 137.

common values the members of FIDE hold dear. In our modern society, European cooperation is not just an option; it is a necessity.

In keeping with good practice and tradition, the XXIX FIDE Congress addresses three main topics for which distinguished General Rapporteurs have been invited to draft a questionnaire on the current relevant legal issues on a European and national level. Rapporteurs from the FIDE Members Associations and prominent experts from the EU institutions have responded with country and institutional reports. Based on this input, the General Rapporteurs compiled a General Report on each topic. You will find all the reports in the FIDE XXIX Congress Publications

While in the early days the Commission's Legal Service would ask FIDE to report on certain questions,[5] the current selection of the three main topics is the result of lively discussions. The organisers of the FIDE XXIX Congress took advantage of valuable contributions from the FIDE Steering Committee, by bringing together the Netherlands academic community and benefiting greatly from the input from practitioners, as well as FIDE members, colleagues and friends in the European Institutions and Member States. The three topics under discussion at the FIDE 2020 Congress revisit some of the classic tenets of EU law, whilst bringing to the table new questions that are triggered by the needs of modern society. Our aim has been to appeal to both specialists and general EU lawyers.

The topics that were selected for the FIDE 2020 Congress are the following:

1. National Courts and the Enforcement of EU Law: The Pivotal Role of National Courts in the EU Legal Order
2. The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection
3. EU Competition Law and the Digital Economy: Protecting Free and Fair Competition in an Age of Technological (R)evolution

The XXIX FIDE Congress Publications are the result of the work of a great variety of EU jurists who, in true European spirit, joined efforts to provide the General Rapporteurs with answers to their questionnaires in various national reports. The General Rapporteurs have compared, evaluated and brought together the insights from the national reports in their General Reports. Together with the Institutional Reports written by experts from the Institutions, and a special report on the EFTA Court, the Congress Publications thus present the state of the art on the three topics of the XXIX FIDE Congress.

European Union law cannot be considered in isolation. To foster a multidisciplinary law-in-context approach, European thinkers from other disciplines – historians, political scientists and economists – have been actively invited to contribute to sessions of the XXIX FIDE Congress to reflect on the way ahead. After years of turmoil, the question poses itself:

5 Rasmussen, 2012, p. 384.

will Europe muddle through, or is there reason to hope for a new European *réveil*? For a Europe that can lead the way in a Green Revolution, that remains a champion of fundamental rights protection and that fosters growth and innovation?

The FIDE 2020 Congress also looks at the critical role national and European judges – who in many Member States function under increased scrutiny and pressure – play in safeguarding the very foundations upon which our legal order was built: the values listed in the Treaty on European Union.

The book that you are currently holding – or reading off your screen – serves to prove that FIDE cherishes tradition but embraces the future. From the outset, we have sought to involve a new generation of European lawyers. Renaming the PhD seminar as the 'Young FIDE Seminar' reflects the ambition to draw in young EU lawyers from a broad range of professional backgrounds. For the first time also young rapporteurs have been asked to report to the FIDE Congress on the discussions at the Young FIDE Seminar.

We are delighted that once more the Congress proceedings will be available to the general public through open access. We extend a heartfelt thank you to all our rapporteurs, our editors and our publisher for making this publication possible. Likewise, we would like to take this opportunity to thank all the volunteers, speakers, sponsors, our Congress Bureau and all those who have in one way or the other contributed to the realisation of the XXIX FIDE Congress in The Hague. We hope that FIDE will continue to inspire, to unite and to prepare for a common European future.

The FIDE 2020 Board
Corinna Wissels (President), Member of the Administrative Jurisdiction Division of the Dutch Council of State
Marleen Botman (Social Programme Officer), Attorney-at-law at Pels Rijcken & Droogleever Fortuijn
Herman van Harten (Secretary General), Judge at the District Court of The Hague
Marlies Noort (Treasurer), Agent before the Court of Justice of the EU, Dutch Ministry of Foreign Affairs
Jorrit J. Rijpma (Scientific Programme Officer), Jean Monnet Professor, Leiden Law School

Introduction from the Editor

Before you lies volume 2 of the XXIX FIDE Congress Publications, bringing together the General, Institutional and National reports on the topic of the new EU data protection regime.

On 25 May 2018, the EU's new regulatory framework for the protection of personal data entered into force. It covers the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data under the General Data Protection Regulation (GDPR) and the processing of personal data by competent authorities for the purposes of criminal justice under the so-called Law Enforcement Directive.

Albeit it a very specialised area of EU law, it raises general questions of EU regulation, governance, enforcement and fundamental rights protection. It is a dynamic area in which the stakes are high and the Court of Justice of the European Union has showed willingness to show its teeth.

It is an area that directly affects businesses and the lives of people. In an increasingly digitised world, personal data constitute a commodity, a threat to privacy, as well as an opportunity for innovation and growth. Almost thirty years after the first legally binding international instrument in the field of data protection, the Council of Europe's Convention 108 for the protection of individuals with regard to automatic processing of personal data was opened for signature, historian Yuval Noah Harari labelled *datism*, the "universal narrative that legitimises the authority of algorithms and Big Data" an existential threat to humankind.[1]

Importantly, the effects of the EU's data protection regime are felt well beyond the borders of the European Union. Not only do the new rules have a global reach, they have also acted, in the words of the late European Data Protection Supervisor Giovanni Buttarelli, as "a clarion call for a new global digital gold standard."[2] Moreover, the EU regime is not just forming a blue print for the regulation of data processing around the world, it is also fuelling further initiatives at EU level for the ethical regulation of technology, data and artificial intelligence.[3]

This work is a first attempt to take stock of the implementation, application and interpretation of the EU's new regulatory framework for data protection. As such it presents

1 Y.N. Harari, *Homo Deus: A Brief History of Tomorrow*, London, Penguin, 2017, p. 428.

2 G. Buttarelli, 'The EU GDPR as a clarion call for a new global digital gold standard, *International Data Privacy Law*, Vol. 6, No 2, 2016, p. 77.

3 See for instance the establishment of a High Level Expert Group on Artificial Intelligence by the European Commission: ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence, visited 1 February 2020.

the reader with a unique comparative perspective and state of the art overview of the EU's data protection rules in the Member States, the EEA and Switzerland. The General Rapporteur, Orla Lynskey, and the Institutional Rapporteurs Herke Kranenborg and Anna Buchta, have brought together the findings of the national reports, as well as have given an overview of developments at EU level in their respective reports.

As editor of this volume I have had the honour and privilege of reading all reports prior to the FIDE congress and to have been in close contact with many of the experts in this field who have contributed to this publication. I would like to thank them for their hard work and patience in handling the deadlines and numerous requests for additional editing or information. A special word of thanks also goes to Carina van Os for her editorial assistance.

In the words of former Justice Commissioner Vera Jurová the GDPR is "still […] a baby that is growing fast and is doing well. But we need to continue to nurture it well."[4] May this edited volume serve as food for thought.

Jorrit J. Rijpma
Jean Monnet Professor, Leiden Law School

4 Speech Commissioner Jurová, 13 June 2019: www.ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_2999, visited 1 February 2020.

Introduction du Comité Directeur du Congrès de la FIDE 2020

C'est dans un petit bar á Tallinn en 2012, tard dans la nuit, qu'un groupe de juristes néerlandais, en visite au congrès biennal de la Fédération Internationale pour le Droit Européen (FIDE) se tenant en Estonie, a évoqué l'idée audacieuse d'organiser ce congrès au Pays-Bas. Huit années plus tard, l'Association Néerlandaise de Droit Européen (NVER – Nederlandse Vereniging voor Europees Recht) a l'honneur d'accueillir les membres de la FIDE à La Haye pour la vingt-neuvième édition de ce congrès ou, plus exactement, de les accueillir à nouveau à La Haye. En effet, la FIDE s'est déjà réunie deux fois dans la ville où siège le gouvernement néerlandais: en 1963 et en 1984. À l'instar de l'Union elle-même, La Haye a changé depuis 1984. Elle a grandi, sa *skyline* s'est transformée et sa position de ville internationale de la paix et de la justice s'est consolidée, notamment avec la présence d'Europol et Eurojust.

L'influence de la FIDE, tant l'organisation elle-même que ses membres, sur le développement du droit européen est bien connue.[1] Dès son commencement, la FIDE a formé un réseau transnational unique rassemblant les acteurs clef qui ont constitué la base du « nouvel ordre juridique »,[2] façonné le droit européen en une véritable discipline autonome et légitimé, lors des premières conférences à La Haye en 1963 et Paris en 1965, « l'interprétation constitutionnelle du droit européen » retenue par la Cour de justice.[3]

Si au début des années 1960, le droit européen n'avait pas encore atteint son plein potentiel, les personnes participant au congrès de 1984 considéraient certainement que les principes de l'effet direct et de la primauté étaient bien établis au moment même où les Communautés européennes s'embarquaient sur le projet, initié par Jacques Delors, de marché intérieur. En revanche, ils n'auraient pas pu imaginer la croissance exponentielle dans les services et les effets aussi formidables que perturbants d'Internet et des nouvelles technologies. En 2020, après les années de crise qui ont fait trembler les fondations mêmes de l'Union, il semble que celle-ci ait à nouveau besoin que la FIDE agisse comme « l'aile

1 J. Laffranque, « FIDE – Uniting Great Minds of European Law: 50 Years of the International Federation for European Law », *Juridica International XVIII,* 2011, p. 173 à 181. Voir également S. Lee Mudge et A. Vauchez, « *Building Europe on a Weak Field: Law, Economics, and Scholarly Avatars in Transnational Politics* » *AJS V*ol. 118, n° 2, 2012, p. 449 à 492. L'équipe organisant le Congrès de la FIDE en Espagne a fait un travail remarquable en rendant une grande partie des archives de la FIDE accessible à ses membres: https://www.fide-europe.org/members-login/, page consultée le 1er février 2020.

2 Arrêt du 5 février 1963, van Gend & Loos (26/62, EU:C:1963:1).

3 M. Rasmussen, « Establishing a Constitutional Practice of European Law: The History of the Legal Service of The European Executive, 1952-65 », *Contemporary European History* Vol. 21 n° 3. 2012, p. 395.

marchante de l'armée des juristes européens »,[4] afin de comprendre, expliquer et défendre une Union fondée sur l'État de droit et notamment sur les valeurs communes qui sont chères aux membres de la FIDE. Dans la société moderne, la coopération européenne n'est pas simplement une option, c'est une nécessité.

Comme le veut la tradition, ce XXIXème Congrès de la FIDE abordera trois sujets principaux pour lesquels d'éminents rapporteurs généraux ont été invités à rédiger un questionnaire portant sur les actuelles questions juridiques pertinentes tant au niveau européen qu'au niveau national. Des rapporteurs issus des associations membres de la FIDE et des experts éminents issus des institutions de l'Union ont répondu sous la forme de rapports nationaux et institutionnels. Sur cette base, les rapporteurs généraux ont préparé un rapport général sur chaque thème. Tous les rapports seront disponibles dans les présentes publications du XXIXème Congrès de la FIDE.

Alors qu'aux débuts de la FIDE, le service juridique de la Commission lui demandait de rendre compte de certaines questions,[5] de nos jours le choix des trois principaux sujets est le résultat de vives discussions. Les organisateurs du XXIXème Congrès de la FIDE ont profité des précieuses contributions du comité directeur de la FIDE en rassemblant la communauté universitaire des Pays-Bas et en tirant un grand avantage de l'apport des praticiens, de même que des membres de la FIDE, collègues et amis dans les institutions européennes et les États membres. Les trois thèmes qui seront discutés lors du Congrès de la FIDE 2020 revisitent certains des thèmes classiques du droit de l'Union tout en y incluant de nouvelles problématiques qui sont nées des besoins de la société moderne. Nous avons souhaité faire appel autant aux spécialistes qu'aux généralistes du droit de l'Union.

Les sujets choisis pour le Congrès de la FIDE 2020 sont les suivants:

1. Les juridictions nationales et l'application du droit de l'Union: le rôle central des juridictions nationales dans l'ordre juridique de l'Union;
2. Le nouveau régime de protection des données de l'Union: la fixation de normes mondiales pour le droit à la protection des données à caractère personnel;
3. Le droit de la concurrence de l'Union et l'économie numérique: la protection d'une concurrence libre et non faussée à l'heure d'une (r)évolution technologique.

Les publications du XXIXème Congrès de la FIDE résultent du travail d'un grand nombre de juristes de droit de l'Union qui, dans le plus pur esprit européen, ont uni leurs forces pour répondre dans leurs rapports nationaux aux questionnaires des rapporteurs généraux. Les rapporteurs généraux ont comparé, évalué et rassemblé les éclairages des différents

4 A. de Vreese, « Droit communautaire et droit national », 14 *Cahiers de Bruges* Vol. 14, n° 399, 1965, cité dans: A. Vauchez, « *Brokering Europe: Euro-Lawyers and the Making of a Transnational Polity* », Cambridge University Press, Cambridge, 2015, p. 137.

5 Rasmussen, 2012, p. 384.

rapports nationaux dans leurs rapports généraux. Avec les rapports institutionnels, rédigés par des experts des institutions, et un rapport spécial de la Cour AELE, les publications du Congrès présentent, sous l'éclairage le plus récent, les trois sujets choisis pour le XXIXème Congrès de la FIDE.

Le droit de l'Union européenne ne peut pas être pris de façon isolée. Pour promouvoir une approche pluridisciplinaire qui place le droit dans son contexte, des penseurs européens issus d'autres disciplines – historiens, politologues et économistes – ont été activement invités à contribuer aux sessions du XXIXème Congrès de la FIDE afin de réfléchir à la route qui se présente devant nous. Après des années de trouble, une question se pose. L'Europe continuera-t-elle à avancer en pataugeant ou existe-t-il des raisons d'espérer qu'un réveil européen ait lieu? Peut-on espérer une Europe qui montre la voie vers une révolution écologique, qui demeure une championne de la protection des droits fondamentaux et qui encourage la croissance et l'innovation?

Le Congrès de la FIDE 2020 se penche également sur le rôle critique que jouent les juges nationaux et européens – qui dans de nombreux États membres font l'objet d'un examen approfondi et d'une pression grandissante – dans la protection des fondements mêmes sur lesquels notre ordre juridique est construit, à savoir les valeurs énumérées dans le traité sur l'Union européenne.

Le livre que vous avez entre les mains – ou que vous lisez sur un écran – est la preuve que la FIDE chérit la tradition tout en embrassant l'avenir. Depuis le commencement de cette aventure, nous avons cherché à impliquer une nouvelle génération de juristes européens. Le fait d'avoir renommé le séminaire doctoral en « Young FIDE Seminar » reflète notre ambition d'attirer de jeunes juristes en droit européen issus de parcours professionnels variés. De même, c'est la première fois qu'il a été demandé à de « jeunes rapporteurs » de présenter, lors du Congrès de la FIDE, les discussions qui ont eu lieu lors du Young FIDE Seminar.

Nous nous réjouissons qu'une fois de plus les travaux du Congrès soient mis à la disposition du public en accès libre. Nous remercions chaleureusement tous nos rapporteurs, nos éditeurs et notre maison d'édition pour avoir permis la publication du présent ouvrage. De même, nous remercions tous les bénévoles, orateurs, sponsors, le Bureau du Congrès et tous ceux qui, d'une manière ou d'une autre, ont contribué à la réalisation du XXIXème Congrès de la FIDE à La Haye. Qu'il nous soit permis d'espérer que la FIDE continuera à inspirer, unifier et préparer un futur européen commun.

Le comité directeur du Congrès de la FIDE 2020
Corinna Wissels (Présidente), membre de la section du contentieux administratif du Conseil d'État néerlandais
Marleen Botman (Chargée du programme social), avocate au cabinet Pels Rijcken & Droogleever Fortuijn

Herman van Harten (Secrétaire Général), juge au tribunal de première instance de La Haye
Marlies Noort (Trésorière), agent du ministère néerlandais des affaires étrangères devant la Cour de justice de l'Union européenne
Jorrit Rijpma (Chargé du programme scientifique), professeur Jean Monnet, faculté de droit de l'université de Leyde

Introduction de l'Éditeur

Vous avez devant vous le volume 2 des publications du XXIXème Congrès de la FIDE qui rassemble le rapport général et les rapports institutionnels et nationaux sur le thème du nouveau régime de protection des données de l'Union. Le nouveau cadre réglementaire de l'Union pour la protection des données à caractère personnel est entré en vigueur le 25 mai 2018. Il couvre la protection des personnes physiques en ce qui concerne le traitement de données à caractère personnel et les règles en matière de libre circulation des données à caractère personnel en application du règlement général sur la protection des données (règlement 2016/679, ci-après le « RGPD »), ainsi que le traitement, par les autorités compétentes, de données à caractère personnel à des fins d'enquêtes pénales en application de la directive sur l'application de la législation (directive 2016/680, ci-après la « DAL »).

Bien qu'il s'agisse d'un domaine très spécialisé du droit de l'Union, il soulève des questions générales en termes de réglementation de l'Union, de gouvernance, d'application et de protection des droits fondamentaux. C'est un domaine dynamique dans lequel les enjeux sont élevés et la Cour de justice de l'Union européenne a d'ailleurs montré qu'elle était prête à montrer les dents.

C'est un domaine qui touche directement la vie des gens et des entreprises. En effet, dans un monde de plus en plus numérique, les données à caractère personnel constituent tout à la fois une marchandise, une menace pour la vie privée et une chance pour l'innovation et la croissance. Presque trente ans après l'ouverture à la signature du premier instrument international juridiquement contraignant dans le domaine de la protection des données, à savoir la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, l'historien Yuval Noah Harari a inventé le terme « dataïsme » pour décrire le « discours universel qui légitime l'autorité des algorithmes et des mégadonnées » et qui constitue, selon lui, une menace existentielle pour l'humanité.[1]

Il importe de préciser que les effets du régime de l'Union en matière de protection des données se font ressentir bien au-delà des frontières de l'Union européenne. Non seulement les nouvelles règles ont une portée mondiale, mais surtout elles ont agi, pour reprendre les mots de feu Giovanni Buttarelli, ancien contrôleur européen de la protection des données, « comme un appel de clairon pour l'établissement d'un nouvel étalon-or numérique mondial ».[2] En outre, non seulement le régime de l'Union constitue un modèle pour la réglementation du traitement des données dans le monde entier, mais il alimente

1 Y.N. Harari, *Homo Deus: A Brief History of Tomorrow,* Penguin, 2017, p. *428*

2 G. Buttarelli, « The EU GDPR as a clarion call for a new global digital gold standard », *International Data Privacy Law*, Vol. 6, n° 2, 2016, p. 77.

également d'autres initiatives au niveau de l'Union pour la réglementation éthique des technologies, des données et de l'intelligence artificielle.[3]

Le présent volume est une première tentative d'inventorier la mise en œuvre, l'application et l'interprétation du nouveau cadre réglementaire de l'Union pour la protection des données. En tant que tel, il offre au lecteur une perspective comparative unique et une vision d'ensemble et à jour des règles européennes de protection des données dans les États membres, l'AELE et la Suisse. Dans leurs rapports respectifs, la rapporteure générale Orla Lynskey et les rapporteurs institutionnels, Herke Kranenborg et Anna Buchta, ont rassemblé les conclusions des rapports nationaux et ont donné une vue d'ensemble des évolutions au niveau de l'Union.

En ma qualité d'éditeur du présent volume, j'ai eu l'honneur et le privilège de lire tous les rapports avant le Congrès et d'être en contact étroit avec un grand nombre des experts de ce domaine qui ont contribué à cette publication. Je souhaite les remercier pour leur travail assidu et leur patience face aux délais à respecter et aux diverses demandes de révision ou d'informations supplémentaires. J'aimerais aussi remercier tout particulièrement Carina van Os pour l'assistance rédactionnelle qu'elle a fourni.

Pour reprendre les propos de M^{me} Věra Jourová, ancienne Commissaire européenne à la Justice, le RGPD est « encore […] un bébé qui grandit vite et est en bonne santé, mais il faut que nous continuions à bien le nourrir ».[4] Que le présent volume puisse constituer un carburant pour cette réflexion.

Jorrit J. Rijpma
Professeur Jean Monnet, faculté de droit de l'université de Leyde

3 Voir, par exemple, la mise en place par la Commission européenne d'un groupe d'experts de haut niveau sur l'intelligence artificielle: ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence, page consultée le 1er février 2020.

4 Discours de M^{me} la Commissaire européenne Věra Jourová, 13 juin 2019: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_2999, page consultée le 1er février 2020.

Begrüssung durch das Organisationskomitee von FIDE 2020

Es war in einer kleinen Kneipe im Jahr 2012 am späten Abend als die Idee geboren wurde, den FIDE-Kongress in die Niederlande zu holen. Eine Gruppe niederländischer Juristinnen und Juristen, die an dem alle zwei Jahre stattfindenden Kongress der Internationalen Föderation für Europarecht (FIDE) – in 2012 in Estland – teilnahmen, hatte damals diese kühne Idee. Acht Jahre später hat die Niederländische Vereinigung für das Europarecht (NVER) die Ehre, die FIDE-Mitglieder in Den Haag zum XXIX FIDE-Kongress zu begrüßen. Oder besser: Sie zum erneuten Mal in Den Haag willkommen zu heißen. Zweimal zuvor tagte FIDE in der Stadt, die gleichzeitig niederländischer Regierungssitz ist: 1963 und 1984. Ähnlich wie die Europäische Union selbst hat sich Den Haag seit 1984 stark verändert. Die Stadt ist gewachsen, ihre Skyline hat sich gewandelt und sie hat ihre Stellung als internationale Stadt des Friedens und der Gerechtigkeit gefestigt, auch dank der Präsenz von Europol und Eurojust.

Der Einfluss von FIDE als Organisation sowie von ihren Mitgliedern auf die Entwicklung des EU-Rechts ist gut dokumentiert.[1] Von Anfang an bildete FIDE einen einzigartigen, länderübergreifenden Verbund, der wichtige Akteure zusammenbrachte, die am Fundament der "neuen Rechtsordnung"[2] arbeiteten, die das Europarecht als eigenständige Disziplin ausgestalteten und die schließlich das "verfassungsmäßige" Verständnis des Gerichtshofs vom EU-Recht auf den ersten Konferenzen in Den Haag (1963) und Paris (1965) legitimierten.[3]

Während das Europarecht Anfang der 1960er Jahre noch lange nicht sein volles Potential ausgeschöpft hatte, mögen die Teilnehmerinnen und Teilnehmer des FIDE-Kongresses von 1984 den Vorrang und die direkte Wirkung des EU-Rechts als weitgehend geklärt angesehen haben, zu einem Zeitpunkt, an dem die Europäischen Gemeinschaften das Binnenmarktprojekt von Jacques Delors in Angriff nehmen sollten. Gleichzeitig konnten sich diese Teilnehmerinnen und Teilnehmer das exponentielle Wachstum im

1 J. Laffranque, 'FIDE – Uniting Great Minds of European Law: 50 Years of the International Federation for European Law', *Juridica International XVIII,* 2011, S. 173-181. Siehe auch: S. Lee Mudge & A. Vauchez, *'Building Europe on a Weak Field: Law, Economics, and Scholarly Avatars in Transnational Politics' AJS* 118 (2012), Ausgabe 2, S. 449-492. Die spanische FIDE-Organisation des Jahres 2010 hat hier eine exzellente Arbeit geleistet, indem sie einen Großteil des FIDE-Archivs für Mitglieder zugänglich gemacht hat: https://www.fide-europe.org/members-login/, besucht am 1 Februar 2020.

2 Urteil vom 5 Februar 1963, Entscheidung 26/62, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*, ECLI:EU:C:1963:1.

3 M. Rasmussen, 'Establishing a Constitutional Practice of European Law: The History of the Legal Service of The European Executive, 1952-65, *Contemporary European History* 21 (2012), Ausgabe 3, S. 395.

Dienstleistungsbereich und die spannenden – teilweise auch mit Gefahren behafteten – Auswirkungen des Internets sowie neuer Technologien gewiss nicht vorstellen. Im Jahr 2020, nach langen Jahren verschiedenster Krisen, die die EU in ihren Grundfesten erschüttert haben, scheint die Europäische Union FIDE erneut zu benötigen, damit diese erneut als "wheeling flank of the army of European jurists "[4] handeln kann. Aber auch um eine Union, die auf Rechtsstaatlichkeit und gemeinsamen Werten beruht, welche den FIDE-Mitgliedern sehr am Herzen liegen, besser zu verstehen, sie besser zu erklären und zugleich zu verteidigen. In unserer modernen Gesellschaft ist die europäische Zusammenarbeit nicht mehr nur eine Möglichkeit, sondern vielmehr eine Notwendigkeit.

Guten Traditionen folgend behandelt der XXIX. FIDE-Kongress drei Hauptthemen. Für diese Themen haben namhafte generelle Berichterstatterinnen und Berichterstatter Fragebögen zu aktuellen Rechtsfragen auf europäischer und nationaler Ebene erstellet. Berichterstatterinnen und Berichterstatter der FIDE-Mitgliederverbände und ausgewiesene Expertinnen und Experten der EU-Organe haben diese Fragebögen mit Länderberichten und institutionellen Berichten beantwortet. Auf Grundlage dieses Inputs haben die generellen Berichterstatterinnen und Berichterstatter einen Gesamtbericht zu jedem Thema erstellt. Sie finden alle diese Berichte in den Kongresspublikationen zum XXIX. FIDE-Kongress.

Während in den ersten Jahren noch der Juristische Dienst der Europäischen Kommission FIDE gebeten hatte, über bestimmte Themen und Fragen zu berichten,[5] ist die aktuelle Auswahl der drei Hauptthemen das Ergebnis lebhafter Diskussionen. Die Organisatoren des XXIX. FIDE-Kongresses nutzten die sehr hilfreichen Beiträge die durch das FIDE-Präsidium, durch den niederländischen akademischen Verbund, sowie durch Praktikerinnen und Praktiker, FIDE-Mitglieder, Kollegeninnen und Kollegen, sowie Bekannte innerhalb der EU Organe und in den Mitgliedstaaten beigesteuert wurden. Die drei Themen, die auf dem FIDE-Kongress 2020 diskutiert werden, greifen einerseits einige der klassischen Themenfelder des EU-Rechts auf und bringen gleichzeitig neue Fragestellungen, die sich in einer modernen Gesellschaft ergeben, auf den Tisch. Unser Ziel war es stets, sowohl Spezialistinnen und Spezialisten als auch allgemeine EU-Juristinnen und -Juristen anzusprechen.

Die Themen, die für den FIDE-Kongress im Jahr 2020 ausgesucht wurden, lauten:

1. Nationale Gerichte und die Durchsetzung von EU-Recht: Die entscheidende Rolle nationaler Gerichte in der Rechtsordnung der Europäischen Union.
2. Das neue EU-Datenschutzregime: Setzen globaler Standards für das individuelle Recht auf Datenschutz.

---

4 A. de Vreese, 'Droit communautaire et droit national', 14 *Cahiers de Bruges* 14 (1985), Ausgabe 399, zitiert in: A. Vauchez, *'Brokering Europe: Euro-Lawyers and the Making of a Transnational Polity'*, Cambridge University Press, Cambridge, 2015, S. 137.

5 Rasmussen, 2012, S. 384.

3. EU-Wettbewerbsrecht und die Digitalwirtschaft: Schutz von freiem und fairem Wettbewerb in Zeiten von technischer (R)Evolution.

Die Publikationen zum XXIX. FIDE-Kongresses sind das Ergebnis der Arbeit einer Vielzahl von EU-Rechtswissenschaftlerinnen und -Rechtswissenschaftlern, die sich im wahrhaft europäischen Geiste zusammengetan haben, um den generellen Berichterstatterinnen und Berichterstatter durch die verschiedenen nationalen Berichte Antworten auf ihre Fragebögen zu geben. Die generellen Berichterstatterinnen und Berichterstatter haben die Erkenntnisse aus den nationalen Berichten verglichen, ausgewertet und in ihren Generalberichten zusammengeführt. Zusammen mit den institutionellen Berichten, die von Expertinnen und Experten der EU-Organe verfasst wurden, und einem Sonderbericht über den EWR-Gerichtshof stellen die Kongresspublikationen somit den aktuellen Wissensstand zu den drei Themenfeldern des XXIX. FIDE-Kongresses dar.

Das Recht der Europäischen Union kann nicht isoliert betrachtet werden. Um einen fächerübergreifenden "*Law-in-Context*"-Ansatz zu fördern, wurden europäische Denkerinnen und Denker aus anderen Fachbereichen und Disziplinen – insbesondere aus den Bereichen Geschichte, Politikwissenschaft und Wirtschaftswissenschaft – eingeladen, aktiv zu den Sitzungen des XXIX. FIDE-Kongresses beizutragen, um gemeinsam über den anstehenden Weg zu reflektieren. Nach Jahren des Aufruhrs stellt sich die folgende Frage: Wird sich Europa einfach irgendwie durchschlagen oder gibt es Grund zur Hoffnung auf ein neues europäisches Erwachen (einen *„réveil")*? Für ein Europa, das in einer grünen Revolution die Führung übernehmen kann, das sich weiterhin für den Schutz der Grundrechte einsetzt und Wachstum und Innovation fördert?

Der in 2020 stattfindende FIDE-Kongress befasst sich auch mit der kritischen Rolle, die nationale siwue europäische Richterinnen und Richter - die in vielen Mitgliedstaaten unter verstärkter Kontrolle und unter Druck arbeiten - bei der Sicherung der Grundlagen unsere Rechtsordnung spielen: nämlich, der Sicherung der im Vertrag über die Europäische Union aufgeführten Grundwerte.

Der Band, den Sie gerade in den Händen halten - oder gegebenenfalls auch auf Ihrem Bildschirm lesen - dient als Beweis dafür, dass FIDE sowohl die Tradition pflegt als auch die Zukunft im Auge hat. Von Anfang an haben wir versucht, eine neue Generation europäischer Juristinnen und Juristen einzubeziehen. Die Umbenennung des vormaligen Doktorandenseminars in "Young FIDE Seminar" zeugt von dem Bestreben, junge EU-Juristeninnen und -Juristen aus einem breiten beruflichen Spektrum anzusprechen. Zum ersten Mal wurden auch "Junge Berichterstatterinnen und Berichterstatter" gebeten, dem FIDE-Kongress über die Diskussionen während des Young FIDE Seminars zu berichten.

Wir freuen uns sehr, dass die Kongressprotokolle erneut der Öffentlichkeit zugänglich gemacht werden können ("open access"). Wir danken allen unseren Berichterstatterinnen

und Berichterstattern, unseren Bearbeiterinnen und Bearbeitern und dem Verlag recht herzlich für die Ermöglichung dieser Publikation. Ebenso möchten wir diese Gelegenheit nutzen, um allen Freiwilligen, Rednerinnen und Rednern, Sponsoren, dem Kongressbüro und all denjenigen zu danken, die auf die eine oder andere Weise zur Durchführung des XXIX. FIDE-Kongresses in Den Haag beigetragen haben. Wir hoffen, dass FIDE weiterhin inspiriert, vereint und uns auf eine gemeinsame europäische Zukunft vorbereiten wird.

Das FIDE-Organisationskomitee,
Corinna Wissels (Präsidentin), Staatsrat in der Verwaltungsrechtsdivision des Niederländischen Verfassungsrates
Marleen Botman (Koordinatorin des Rahmenprogramms), Rechtsanwältin bei Pels Rijcken & Droogleever Fortuijn
Herman van Harten (Geschäftsführer), Richter am Amtsgericht Den Haag
Marlies Noort (Kassenwartin), Bevollmächtigte vor dem Europäischen Gerichtshof, Außenministerium der Niederlande
Jorrit Rijpma (Koordinator des wissenschaftlichen Programms), Jean Monnet Professor, Universität Leiden, Juristische Fakultät (Leiden Law School)

Vorwort des Bearbeiter

Vor Ihnen liegt Band 2 der XXIX. FIDE-Kongresspublikationen, der die allgemeinen, institutionellen und nationalen Berichte zum Thema der neuen EU-Datenschutzregelung beinhaltet.

Am 25. Mai 2018 trat der neue EU-Rechtsrahmen für den Schutz personenbezogener Daten in Kraft. Er umfasst den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und die Vorschriften über den freien Verkehr personenbezogener Daten gemäß der Allgemeinen Datenschutzgrundverordnung (DSGVO) sowie die Verarbeitung personenbezogener Daten durch zuständige Behörden für die Zwecke der Strafverfolgung gemäß der sogenannten Strafverfolgungsrichtlinie.

Obwohl es sich um einen sehr spezifischen Bereich des EU-Rechts handelt, wirft dieser Themenbereich doch allgemeine Fragen der EU-Regulierung, der Governance, der Durchsetzung und des Schutzes der Grundrechte auf. Es ist ein dynamischer Bereich, in dem viel auf dem Spiel steht und der Gerichtshof der Europäischen Union hat die Bereitschaft erkennen lassen, sprichwörtlich seine Zähne zu zeigen.

Es ist ein Thema, das das Leben der Menschen und auch Unternehmen direkt berührt. In einer zunehmend digitalisierten Welt stellen persönliche Daten gleichzeitig eine Ware, eine Bedrohung der Privatsphäre und eine Chance für Innovation und Wachstum dar. Fast dreißig Jahre nach dem das erste rechtsverbindliche internationale Instrument im Bereich des Datenschutzes zur Ratifikation gestellt wurde, nämlich dem Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, bezeichnet der Historiker Yuval Noah Harari den „Datismus", nämlich die „universelle Erzählung, die die Autorität von Algorithmen und großen Daten legitimiert ", als eine existenzielle Bedrohung für die Menschheit.[1]

Bedeutsam ist ferner, dass die Auswirkungen der EU-Datenschutzregelungen weit über die Grenzen der Europäischen Union hinaus spürbar sind. Die neuen Regeln haben nicht nur eine globale Reichweite, sondern sie fungieren auch, wie der vor Kurzem verstorbene Europäische Datenschutzbeauftragte Giovanni Buttarelli sagte, als "ein Appell für einen neuen globalen digitalen Goldstandard".[2] Darüber hinaus bilden die EU-Regelungen nicht nur eine Anleitung für die Regulierung der Datenverarbeitung global, sondern sie treiben

1 Auf Englisch: „universal narrative that legitimises the authority of algorithms and Big Data"; Y.N. Harari, *Homo Deus: A Brief History of Tomorrow, Penguin, 2017, S. 428*

2 Auf Englisch: „a clarion call for a new global digital gold standard"; G. Buttarelli, 'The EU GDPR as a clarion call for a new global digital gold standard, *International Data Privacy Law* 6 (2016), Ausgabe 2, S. 77.

auch weitere Initiativen auf EU-Ebene für die ethische Regulierung von Technologie, Daten und künstlicher Intelligenz voran.[3]

Dieses Band ist ein Versuch, eine erste Bestandsaufnahme der Umsetzung, Anwendung und Interpretation des neuen EU-Datenschutzrechtsrahmen zu erstellen. Als solches bietet er den Leserinnen und Lesern eine einzigartige vergleichende Perspektive und einen Überblick über den aktuellen Stand der Anwendung der EU-Datenschutzvorschriften innerhalb der Mitgliedstaaten, in dem EWR und in der Schweiz. Die generelle Berichterstatterin, Orla Lynskey, und die institutionellen Berichterstatter, Herke Kranenborg und Anna Buchta, haben in ihren jeweiligen Berichten die Erkenntnisse der nationalen Berichte sowie die entsprechenden Entwicklungen auf EU-Ebene zusammengetragen.

Als Bearbeiter dieses Bandes hatte ich die Ehre und das Privileg, alle Berichte vor dem FIDE-Kongress lesen zu können und stand mit vielen der Expertinnen und Experten dieses Themenbereichs, die zu dieser Publikation beigetragen haben, in engem Kontakt. Ich möchte ihnen für ihre harte Arbeit und ihre Geduld, insbesondere mit Blick auf die Abgabefrist sowie auf verschiedenste Bitten um zusätzliche Bearbeitung oder Anfragen zu zusätzlichen Informationen, danken. Ein besonderes Wort des Dankes gilt auch Carina van Os für ihre redaktionelle Unterstützung.

Nach den Worten der ehemaligen Justizkommissarin Vera Jurová ist das DSGVO „immer noch […] ein Baby, das schnell wächst und dem es gut geht. Aber wir müssen es weiterhin gut ernähren."[4] In diesem Sinne, möge dieser Band als sinnbildliche geistige Nahrung dienen.

Jorrit J. Rijpma
Jean Monnet Professor, Universität Leiden, Juristische Fakultät (Leiden Law School)

3 Siehe, zum Beispiel, die Einrichtung einer High Level Expert Group on Artificial Intelligence durch die Europäische Kommission: ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence, besucht am 1 Februar 2020.

4 Auf Englisch: „still […] a baby that is growing fast and is doing well. But we need to continue to nurture it well."; Rede von Kommissarin Jurova, 13 Juni 2019: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_2999, besucht am 1 Februar 2020.

Questionnaire Topic 2: The New EU Data Protection Regime

General Introduction

The new EU data protection package entered into force in May 2018, following a protracted legislative process. The package comprised a General Data Protection Regulation (Regulation 2016/679, GDPR) and a lesser-known Law Enforcement Directive (Directive 2016/680, LED). The GDPR, in particular, seeks to "Europeanise" data protection law and to render it more effective: by introducing a regulation rather than a directive, an attempt is made to minimise national divergence while significant new avenues for private redress and public enforcement are introduced. Although the responsibility for public enforcement of the framework lies primarily with national supervisory authorities (NSAs), the creation of a new European body with the power to issue authoritative opinions and, in specific cases, binding decisions has a centralising effect on data protection enforcement. The hope is that the changes brought about by the GDPR will ultimately enhance the effectiveness of the EU Charter rights to data protection and privacy. Yet, despite this shift towards a truly European legal framework for data protection, and unusually for a regulation, the GPDR leaves much responsibility to the national legislature, NSAs and courts.

This new regulatory framework raises substantive, procedural and institutional issues that will of interest and relevance to general EU lawyers and those specialising in other fields of substantive EU law.

Those with an interest in procedural and institutional matters will note that the GDPR sets out detailed provisions on remedies, liability and penalties. These provisions specify high administrative fines and provide for the possibility of criminal sanctions, as well as introducing provisions providing for representative actions by non-profit organisations. These detailed remedies, avenues for redress and sanctions will need to be accommodated within the national legal system in a way that is compatible with the general principle of national procedural autonomy. Moreover, the similarities between the enforcement possibilities afforded by the GDPR and those applicable to financial services in the EU (in particular, the power of an EU body to issue decisions binding on national regulators) will not go unnoticed.

From a substantive perspective, the application of the EU Charter rights to data protection and privacy has had a transformative effect on the fundamental rights landscape in Europe. How the EU Charter has impacted upon domestic legal systems in this area as well as the impact of the GDPR on other rights, such as freedom of expression, is therefore

covered in this questionnaire. Furthermore, the CJEU has been pushing the boundaries of the Charter right to respect for privacy in the context of law enforcement. The relevance of this jurisprudence to domestic national security interests, and thus issues of sovereignty, remains contested.

Beyond these broader EU law questions, this questionnaire addresses issues that are specific to the EU data protection framework. Although necessarily drafted in a technical and legalistic manner, these issues are of fundamental societal interest. For example, following the Facebook-Cambridge Analytica scandal, there has been renewed public interest and debate regarding the handling and harvesting of our data by technology giants and the bargain we have entered into with these actors (access to 'free' services in exchange for this personal data processing, addressed in question 5). Similarly, whether individuals should have a right to delete their data from the de facto public record (for instance, a search engine service like Google) when there is a countervailing public interest in this information is hotly contested and addressed in question eight.

The ambition of this questionnaire is to gauge how this new legal framework for data protection has been received by all relevant actors at national level (most notably, Courts; national Parliaments; national supervisory authorities; and civil society). This national data will then be used to inform the discussion of both the specific data protection questions and the general EU law issues that the new legal framework entails.

This being so, this questionnaire is structured around four key areas of inquiry:

A Setting the Scene
B The Reception of Substantive GDPR Provisions in the National Legal Order
C Domestic Enforcement of Data Protection Law
D Data Processing for National Security Purposes

A Setting the Scene

The GDPR is unusual in so far as it is a Regulation that leaves significant scope for the national legislature to avail of the flexibilities incorporated in many provisions.

1 *Please identify and describe the main national legal instruments that have been introduced to implement the GDPR. In particular, outline how these instruments avail of the most notable flexibilities incorporated in the GDPR (in, for example, Article 6(1)(c); Article 23 and 86-90 GDPR) and what oversight role the national supervisory authority (NSA) exercises in relation to these instruments.*

The EU Charter is unique amongst international human rights instruments in so far as it incorporates distinct provisions to protect the right to respect for private life and the right to data protection (Articles 7 and 8 EU Charter).

2 *Does your national legal order differentiate between these rights? Has the EU Charter right to data protection influenced the interpretation of national law?*

B The Reception of Substantive GDPR Provisions in the National Legal Order

While EDPB guidelines should minimise divergence between Member States on the interpretation of the GDPR's substantive provisions, even in this situation the possibility remains that the acceptance of the EDPB's findings remain contested at national level (for instance, by the judiciary; by other relevant regulators; by academics; or, by civil society and the media). It is for this reason that the following questions are asked.

GDPR Responsibilities

Many of the safeguards, or 'principles', relating to data processing remain unchanged from the 1995 Data Protection Directive. Yet, the meaning and practical impact of critical principles remains underdeveloped with limited guidance, to date, from the Court of Justice of the EU (CJEU).

3 *How have data controllers interpreted and applied the principles of 'fair' processing; purpose limitation and 'data minimisation'? Has the NSA applied these principles and have they been interpreted by domestic courts?*

The Article 29 Working Party provided an Opinion on the use of 'legitimate interests' as a legal basis for data processing and, more recently guidelines on the concept of consent (endorsed by the EDPB).

4 *How have these legal bases – 'consent' and 'legitimate interests' – arguably the most significant yet opaque in the digital environment – been interpreted by national courts?*

Most digital services and content offered to Internet users are offered for free-at-the-point-of- access to end-users. This service or content is then subsidised through the provision of online behavioural advertising tailored to the user based on a profile generated through the processing of their personal data. In this way, personal data becomes the indirect counter-performance or 'payment' for the provision of the 'free' digital content

or service. Article 7(4) GDPR stipulates that, in situations where consent is used to justify personal data processing, when assessing whether consent is freely given, utmost account should be taken of whether the performance of a contract is made conditional on consent to the processing of unnecessary data. Similarly, Article 6(1)(b) provides that processing is lawful when 'it is *necessary* for the performance of a contract to which the data subject is party' (emphasis added).

5 *Has there been debate or decision at national level regarding the validity of personal data as 'counter-performance' for the provision of digital content?*

GDPR Rights

The GDPR seeks to render existing rights (such as the right of access to data by the data subjects) more effective by specifying their meaning while introducing one 'brand new right', a right to data portability.

6 *Article 22 provides for a right not to be subject to automated decision-making, including profiling. Article 22(2)(b) allows Member States to introduce legislative measures to ensure this right does not apply in certain situations. Have such legislative measures been introduced and, if so, what measures to safeguard the rights, freedoms and legitimate interests of data subjects do they incorporate?*
7 *How has the right to erasure (Article 17), or its Data Protection Directive predecessor (Directive 95/46 EC, Article 12) been applied at national level by search engines, the NSA or Courts?*
8 *The GDPR allows Member States to legislate to reconcile the right to data protection with freedom of expression (Article 85). Has your state introduced a law pursuant to Article 85(2) GDPR and, if so, how has this been interpreted and applied to date?*

C Domestic Enforcement of Data Protection Law

The GDPR revolutionises the enforcement of data protection in Europe. On the one hand, it introduces a new EU body, the European Data Protection Board (EDPB) with the power to adopt authoritative opinions and, ultimately, even binding decisions on any matter of general application or producing effects in more than one Member State.[1] On the other hand, it introduces an array of new remedies and penalties, including significant administrative sanctions and the possibility for collective redress. The interaction between

1 This results from a combined reading of Article 64(2) and Article 65(1)(c) GDPR.

these new provisions and existing national procedural rules is likely to be complicated. It is against this backdrop that the following questions are asked.

NSAs are the guardians of the GDPR: they are tasked with the role of monitoring its application and contributing to the consistency of such application.

9 *Identify the relevant public authority (or authorities) in your Member State. Outline its composition; the appointment process for members and staff; any additional power or duties the NSA is entrusted with under national law; and, provide relevant details regarding its 'enforcement record' under the GDPR.*

The GDPR provides individuals with a right to lodge a complaint before a supervisory authority and states that the supervisory authority shall inform the complainant on the progress and outcome of that complaint. Some commentators have advocated that supervisory authorities should adopt a 'selective to be effective' approach to complaints by triaging them to focus resources on the most significant (for instance, in terms of scale or legal precedent).

10 *What strategy for complaint-handling is taken by your NSA and what, if any, constraints does domestic law place on such a strategy?*

The GDPR provides Member States with new mechanisms to sanction data protection infringements, including the power to impose corrective measures (Article 58(2)), enhanced administrative fines (Article 83) and the possibility to impose 'other penalties' (Article 84 GDPR).

11 *How have these sanctions been applied by your NSA, and what additional sanctions have been adopted at national level in addition to those explicitly provided for by the GDPR?*

The GDPR provides that data subjects should be compensated for damages suffered for tangible and intangible harm (Article 82).

12 *Has your legal system historically awarded damages for intangible harm (in this area or others)? If so, how are such damages calculated?*

Data processing operations in the online environment in particular can be characterised by information and power asymmetries between data controllers and data subjects. The GPDR seeks to mitigate these asymmetries by providing for the possibility of representative actions pursuant to Article 80 GDPR.

13 *Has your Member State introduced legislative measures to facilitate such representative actions? What role have NGO's played in data protection enforcement in your State and are there any alternative movements emerging at national level (such as personal data cooperatives or unions) to combat such asymmetries?*

As personal data has both an economic and a dignitary value there is an increasing trend for regulators beyond NSAs to intervene in data processing related complaints (for instance, competition authorities and consumer protection authorities). Moreover, in some states new regulatory bodies for the Internet and/or Artificial Intelligence are proposed.

14 *Have these trends been visible in your Member State? In particular, has the NSA cooperated with other regulators or an ombudsperson formally or informally?*

D Data Processing for National Security Purposes

Both the GDPR and the Law Enforcement Directive exclude from their scope of application personal data processing for 'national security' purposes. The Law Enforcement Directive seeks, for the first time, to regulate the domestic data processing operations of law enforcement authorities. The dividing line between law enforcement activities, within the Directive's scope, and national security activities, outside its scope, may therefore give rise to contestation at national level.

15 *Is 'national security' defined in your domestic law or administrative practice? Have national authorities accepted the application of the EU Charter to data retention for national security purposes (following from the* Tele 2 *and* Watson *judgments)?*

Questionnaire Thème 2: Le Nouveau Régime de Protection des Données de l'UE

Introduction générale

Le nouveau paquet de l'Union en matière de protection des données est entré en vigueur en mai 2018 à la suite d'un long processus législatif. Le paquet comprend un règlement général sur la protection des données (règlement 2016/679, ci-après le « RGPD ») et une directive sur l'application de la législation (directive 2016/680, ci-après la « DAL »). Le RGPD vise notamment à « européaniser » le droit en matière de protection des données, ainsi que le rendre plus effectif. L'introduction d'un règlement, au lieu d'une directive, envisage de réduire les divergences nationales en ce qui concerne les dispositions de fond. Également, le RGPD introduit des instruments essentiellement nouveaux pour la mise en vigueur, y compris des recours par des parties privées et des fonctions des autorités de contrôle publics. Bien que la responsabilité pour le contrôle des instruments juridiques fait surtout partie de la mission des autorités de contrôle nationales, la création d'un nouvel organisme européen ayant le pouvoir de rendre des avis ayant de l'effet juridique et, dans les circonstances spécifiques, des décisions contraignantes a la conséquence de centraliser le respect de la protection des données. Il est à espérer que les changements apportés par le RGPD augmenteront au final l'effectivité des droits à la protection des données et au respect de la vie privée prévus par la charte des droits fondamentaux de l'Union européenne (ci-après « la Charte »). Pourtant, malgré cette évolution vers un cadre juridique vraiment européen de la protection des données, et de façon inhabituelle pour un règlement, le RGPD laisse une grande responsabilité au législateur national, aux autorités nationales chargées de la protection des données (ci-après les « autorités nationales ») et aux tribunaux.

Ce nouveau cadre réglementaire soulève des questions procédurales, de fond et des questions institutionnelles qui seront intéressantes tant pour les juristes généraux de droit de l'Union que pour ceux spécialisés dans des domaines spécifiques substantiels du droit de l'Union.

Les personnes ayant un intérêt pour les questions procédurales et institutionnelles remarqueront que le RGPD contient des dispositions particulières concernant les voies de recours, responsabilités et sanctions. Ces dispositions prévoient des amendes administratives élevées et permettent que les états membres introduisent des sanctions pénales. En plus, les états membres sont en mesure de prévoir des actions par des organisations non gouvernementales représentatives. Ces voies de recours, responsabilités et sanctions détaillés devront être adaptées au système juridique national de sorte qu'elles

soient compatibles avec le principe général de l'autonomie procédurale. En outre, les similarités existant entre les possibilités d'exécution forcée prévues par le RGPD et celles applicables aux services financiers dans l'Union (notamment le pouvoir accordé à un organe de l'Union de prendre des décisions contraignantes envers les autorités nationales de régulation) ne passeront pas inaperçues.

Sur le fond, l'application de la Charte à la protection des données et de la vie privée a transformé le paysage des droits fondamentaux en Europe. Le questionnaire couvre donc la façon dont la Charte a modifié les systèmes juridiques internes dans ce domaine, ainsi que l'incidence du RGPD sur d'autres droits tels que la liberté d'expression. En outre, le juge de l'Union a repoussé les limites du droit au respect de la vie privée prévu par la Charte dans le contexte de l'application de la loi. La pertinence de cette jurisprudence pour les intérêts nationaux en matière de sécurité et donc pour les questions de souveraineté reste contestée.

Au-delà de ces questions larges de droit de l'Union, le présent questionnaire traite également de questions spécifiques au cadre de protection des données de l'Union. Bien que ces questions soient rédigées d'une façon nécessairement technico-juridique, ses questions présentent un intérêt sociétal certain. Par exemple, à la suite du scandale Facebook-Cambridge Analytica l'intérêt et le débat publics ont été renouvelés quant à la gestion et la récolte de nos données par des géants technologiques et quant au marché conclu avec ces acteurs (à savoir l'accès à des services « gratuits » en échange du traitement de ces données personnelles, point qui est traité par la question 5). De même, la question de savoir si les particuliers doivent avoir le droit d'effacer leurs données du registre public de fait (par exemple, un service de moteur de recherche comme Google) lorsqu'il existe un intérêt public à accéder à cette information est vivement contestée et sera traitée dans la question 8.

Le présent questionnaire ambitionne d'évaluer la manière dont ce nouveau cadre juridique pour la protection des données a été reçu par les différents acteurs au niveau national (en particulier, les juridictions, les parlements nationaux, les autorités nationales de régulation et la société civile). Ces données nationales seront ensuite utilisées pour éclairer tant la discussion relative aux questions spécifiques en matière de protection des données que celle relative aux questions générales de droit de l'Union que le nouveau cadre réglementaire suscite.

Cela étant, le présent questionnaire est structuré autour de quatre grands sujets:

A Présentation du contexte
B Réception des dispositions de fond du RGPD dans l'ordre juridique national
C Application interne de la législation en matière de protection des données
D Traitement de données pour des motifs de sécurité nationale

A Présentation du contexte

Le RGPD est un règlement atypique en ce qu'il accorde au législateur national une marge significative lui permettant de se prévaloir de la souplesse prévue dans de nombreuses dispositions.

1 *Merci d'identifier et de décrire les principaux instruments juridiques qui ont été introduits pour mettre en œuvre le RGPD. Merci d'exposer notamment la façon dont ces instruments utilisent les principales marges de manœuvre permises par le RGPD [notamment à l'article 6, paragraphe 1, sous c), l'article 23 et aux articles 86 à 90 du RGPD] et de préciser quel rôle de surveillance joue l'autorité nationale de contrôle concernant ces instruments.*
La Charte est un cas unique parmi les instruments internationaux de protection des droits humains en ce qu'elle contient des dispositions distinctes pour protéger le droit au respect de la vie privée et le droit à la protection des données (articles 7 et 8 de la Charte).

2 *Votre ordre juridique national établit-il une distinction entre ces deux droits? Le droit à la protection des données prévu par la Charte a-t-il influencé l'interprétation de votre droit national?*

B Réception des dispositions de fond du RGPD dans l'ordre juridique national

Même si les lignes directrices du Comité européen de la protection des données (ci-après le « CEPD ») devraient minimiser les divergences entre États membres, la possibilité demeure que les conclusions du CEPD soient contestées au niveau national (par le pouvoir judiciaire, par d'autres autorités de régulation, par des universitaires ou encore par la société civile ou les médias). C'est pourquoi les questions ci-dessous sont posées.

Obligations au titre du RGPD

Un grand nombre des garanties ou « principes » relatifs au traitement des données reste inchangé par rapport à la directive de 1995 sur la protection des données. Pourtant, la signification et l'incidence pratique de principes critiques demeurent insuffisantes et, les indications fournies à ce jour, par le juge de l'Union, sont limitées.

3 *De quelle façon les responsables du traitement des données ont-ils interprété et appliqué les principes du « traitement loyal », de limitation des finalités et de minimisation des données? L'autorité nationale de contrôle a-t-elle appliqué ces principes et ces derniers ont-ils été interprétés par les juridictions internes?*

Le groupe de travail de l'article 29 a rendu un avis sur l'utilisation des « intérêts légitimes » comme fondement juridique pour le traitement des données, ainsi que des lignes directrices sur le consentement (approuvé par le Comité européen de la protection des données)

4 *De quelle façon ces fondements juridiques – le « consentement » et les « intérêts légitimes » – qui sont sans doute les plus importants (malgré le flou qui les entoure dans un environnement numérique) sont-ils interprétés par les juridictions nationales?*

La grande partie des services et contenus numériques offerts aux utilisateurs d'Internet sont accessibles gratuitement par l'utilisateur final. Ce service ou contenu est ensuite subventionné au moyen d'une publicité comportementale en ligne personnalisée à l'utilisateur sur la base d'un profil généré par le traitement de ses données personnelles. Ainsi, les données personnelles deviennent la contrepartie ou la « rémunération » de la fourniture du contenu ou service numérique « gratuit ». L'article 7, paragraphe 4, du RGPD prévoit que lorsque le consentement est utilisé pour justifier un traitement de données personnelles, au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir si l'exécution d'un contrat est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. De même, l'article 6, paragraphe 1, sous b), dispose que le traitement est licite lorsqu'il « est *nécessaire* à l'exécution d'un contrat auquel la personne concernée est partie » (mise en italique par nos soins).

5 *Un débat a-t-il eu lieu ou une décision a-t-elle été prise, au niveau national, quant à la validité du transfert de données personnelles comme « contrepartie » à la fourniture de contenus numériques?*

Droits au titre du RGPD

Le RGPD vise à rendre plus effectifs des droits existants (comme le droit d'accéder à ses propres données personnelles) en précisant leur signification et en introduisant un nouveau droit, à savoir le droit à la portabilité des données.

6 *L'article 22 prévoit le droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé, y compris le profilage. L'article 22, paragraphe 2, sous b), autorise les États membres à légiférer pour écarter l'application de ce droit, dans certaines circonstances. Une telle législation a-t-elle été mise en place et, dans l'affirmative, quelles mesures pour la sauvegarde des droits, libertés et des intérêts légitimes de la personne concernée contient-elle?*

7 *Le droit à l'effacement (article 17), ou son prédécesseur issu de la directive de 1995 sur la protection des données (article 12 de la directive 95/46/CE,), comment a-t-il été appliqué au niveau national par les moteurs de recherche, les autorités nationales de contrôle ou les tribunaux?*

8 *Le RGPD permet aux États membres de légiférer pour concilier le droit à la protection des données et le droit à la liberté d'expression (article 85). Votre État a-t-il adopté une loi au titre de l'article 85, paragraphe 2, du RGPD et, dans l'affirmative, comment a-t-elle été interprétée et appliquée jusqu'à présent?*

C Application interne de la législation en matière de protection des données

Le RGPD révolutionne la mise en œuvre de la protection des données en Europe. D'une part, il crée un nouvel organe de l'Union, à savoir le Comité Européen de la Protection des Données qui est compétent pour adopter des avis avec effet juridique et, ultérieurement, des décisions contraignantes concernant toute question d'application générale ou produisant des effets dans plusieurs États membres[1]. D'autre part, il introduit un éventail de nouvelles voies de recours et de nouvelles sanctions, notamment des sanctions administratives significatives et la possibilité de recours collectifs. L'articulation entre ces nouvelles dispositions et les règles procédurales nationales existantes risque de se révéler complexe. C'est dans ce contexte que les questions suivantes sont posées.

Les autorités nationales de contrôle sont les gardiens du RGPD: elles sont chargées de contrôler son application et de contribuer à la cohérence de cette application.

9 *Veuillez, d'abord, identifier l'autorité (ou les autorités) publique pertinente dans votre État membre. Merci, ensuite, d'exposer brièvement sa composition, la procédure d'embauche du personnel et de préciser si, en application du droit national, des pouvoirs ou obligations additionnels sont confiés à l'autorité nationale de contrôle. Veuillez, enfin, donner les détails pertinents concernant son bilan en ce qui concerne la mise en œuvre du RGPD.*

Le RGPD accorde aux particuliers le droit d'introduire une réclamation auprès d'une autorité de contrôle et précise que cette autorité doit informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête. Certains commentateurs ont estimé que

1 Cela résulte d'une lecture combinée de l'article 64, paragraphe 2, et de l'article 65, paragraphe 1, sous c), du RGPD.

les autorités de contrôle devraient retenir, au nom d'une plus grande efficacité, une approche sélective des réclamations. Selon eux, il conviendrait de trier les réclamations et de concentrer les ressources des autorités sur les plus importantes (par exemple, en termes de taille ou de précédent judiciaire qui sera fixé à cette occasion).

10 *Quelle stratégie a retenu votre autorité nationale de contrôle, en termes de gestion des réclamations, et quelles contraintes éventuelles le droit national a-t-il imposé à cette stratégie?*

Le RGPD prévoit au profit des États membres de nouveaux mécanismes permettant de sanctionner les infractions aux règles sur la protection des données, y compris le pouvoir d'imposer des mesures correctrices (article 58, paragraphe 2,), des amendes administratives plus élevées (article 83) et la possibilité d'infliger d' « autres sanctions » (article 84).

11 *Comment ces sanctions ont-elles été appliquées par votre autorité nationale de contrôle et quelles sanctions additionnelles ont été adoptées au niveau national en plus de celles prévues expressément par le RGPD?*

Le RGPD prévoit que les personnes concernées ayant subi un dommage matériel ou moral ont le droit d'obtenir réparation du préjudice subi (article 82).

12 *La réparation d'un dommage moral est-elle possible dans votre système juridique (dans ce domaine ou dans un autre)? Si tel est le cas, comment les dommages et intérêts alloués sont-ils calculés?*

Les opérations de traitement de données en ligne se caractérisent par des asymétries, en termes de pouvoirs et d'informations, entre les responsables du traitement des données et les personnes concernées par ce traitement. Le RGPD cherche à atténuer ces asymétries en prévoyant à son article 80 la possibilité d'actions représentatives.

13 *Votre État membre a-t-il légiféré pour faciliter ces actions représentatives? Quel rôle ont joué les ONG dans l'application des règles en matière de protection des données dans votre État et existe-t-il des mouvements alternatifs nouveaux au niveau national (comme par exemple des syndicats ou coopératives dédiés à la protection des données à caractère personnel)?*

Dans la mesure où les données personnelles ont à la fois une valeur économique et une valeur en termes de dignité humaine, il existe une tendance grandissante chez certains régulateurs autres que les autorités nationales de contrôle à intervenir dans les réclamations

relatives à un traitement de données (par exemple, les autorités de concurrence ou les autorités en charge de la protection des consommateurs).

14 *Cette tendance existe-t-elle dans votre État membre? En particulier, votre autorité nationale de contrôle a-t-elle collaboré, formellement ou informellement, avec d'autres autorités de régulation ou avec le médiateur?*

D Traitement de données pour des motifs de sécurité nationale

Le RGPD et la DAL excluent de leur champ d'application le traitement des données personnelles pour des motifs de « sécurité nationale ». La DAL a pour objet de réglementer, pour la première fois, les opérations internes de traitement des données par les services répressifs. La ligne de partage entre, d'une part, les activités répressives relevant du champ d'application de la directive et, d'autre part, les activités relatives à la sécurité nationale ne relevant pas de son champ d'application, pourrait donner lieu à des contestations au niveau national.

15 *La notion de « sécurité nationale » est-elle définie dans votre droit national ou dans la pratique administrative interne? Les autorités nationales ont-elles accepté d'appliquer la Charte à la conservation des données pour des motifs de sécurité nationale [à la suite de l'arrêt du 21 décembre 2016,* Tele2 Sverige *et* Watson e.a. *(C–203/15 et C–698/15, EU:C:2016:970)]?*

Fragebogen Thema 2: Das Neue EU-Datenschutzregime

Allgemeine Einführung

Nach einem langjährigen Gesetzgebungsprozess ist im Mai 2018 das neue EU-Datenschutzpaket in Kraft getreten. Das Paket umfasst die EU-Datenschutzgrundverordnung (Verordnung 2016/679, nachfolgend: DSGVO) sowie die weniger bekannte Umsetzungsrichtlinie für den Bereich Justiz und Inneres (Richtlinie 2016/680, nachfolgend: JI-Richtlinie). Ziel, insbesondere der DSGVO, ist sowohl eine Europäisierung als auch ein effektiverer Datenschutz: Durch die Einführung einer Verordnung anstelle einer Richtlinie wurde der Versuch unternommen nationale Abweichungen zu minimieren, während gleichzeitig neue Möglichkeiten privater Abhilfe sowie öffentlich-rechtlicher Rechtsdurchsetzung eingeführt werden. Obwohl die Verantwortung für die öffentlich-rechtliche Durchsetzung des Rechtsrahmens in erster Linie bei den nationalen Aufsichtsbehörden liegt, hat die Gründung einer neuen EU-Datenschutzbehörde, mit der Befugnis maßgebliche Stellungnahmen zu verfassen sowie in bestimmten Fällen sogar bindende Entscheidungen zu treffen, einen zentralisierenden Effekt für die datenschutzrechtliche Rechtsdurchsetzung. Ferner besteht die Hoffnung, dass durch die mit der DSGVO eingeführten Veränderungen schlussendlich das Recht auf Datenschutz und das Recht auf Privacy – niedergelegt in der EU-Grundrechtecharter – effektiver geschützt werden können. Trotz dieser Entwicklung hin zu einem einheitlichen EU-Rechtsrahmen im Datenschutz, überträgt die DSGVO, anders als bei EU-Verordnungen eigentlich üblich, den nationalen Gesetzgebern, Datenschutz-Aufsichtsbehörden und Gerichten weitreichende Verantwortung.

Dieser neue Regulierungsrahmen wirft materiell-rechtliche, verfahrensrechtliche und institutionelle Fragen von Bedeutung für allgemeine EU-Juristen sowie Spezialisten in speziellen materiellen EU-Rechtsfeldern auf.

Diejenigen mit einem besonderen Interesse an verfahrensrechtlichen und institutionellen Fragen werden feststellen, dass die DSGVO detaillierte Vorschriften über allgemeine Rechtmittel, Haftungsfragen sowie mögliche Strafen enthält. Diese Vorschriften listen hohe Bußgelder und sehen strafrechtliche Sanktionen sowie Verbandsklagen von gemeinnützigen Organisationen vor. Diese detaillierten allgemeinen Rechtsmittel, Abhilfe- und Sanktionsmöglichkeiten müssen, unter Berücksichtigung mitgliedsstaatlicher Verfahrensautonomie, in die nationale Rechtsordnung integriert werden. Außerdem fällt auf, dass die Durchsetzungsmöglichkeiten unter der DSGVO deutliche Ähnlichkeit mit

den einschlägigen Vorschriften für Finanzdienstleistungen (insbesondere die Befugnisse einer zentralen EU-Einrichtung einheitliche Entscheidungen zu treffen) aufweisen.

Materiell-rechtliche gesehen, hat die Anwendung des Rechts auf Datenschutz und des Rechts auf Privacy, die jeweils in der EU-Grundrechtecharta niedergelegt sind, einen umgestaltenden Effekt auf die *Europäische Grundrechtslandkarte* gehabt. Deshalb behandelt dieser Fragebogen auch den Einfluss, den die EU-Grundrechtecharta auf die nationale Rechtsordnung in diesem Bereich sowie den Einfluss der DSGVO auf andere Grundrechte, einschließlich der Meinungsfreiheit, hat. Darüber hinaus hat der Europäische Gerichtshof (EuGH) die Grenzen des Privatsphäreschutzes im Sinne der EU- Grundrechtecharta im Bereich der Rechtsdurchsetzung verschoben. Die Bedeutung dieser Rechtsprechung für nationale Sicherheitsfragen, und somit auch für die nationale Souveränität, bleibt weiterhin umstritten.

Neben diesen allgemeinen EU-rechtlichen Fragen widmet sich dieser Fragebogen auch bestimmten Problemen, die spezifisch für den EU-Datenschutzrahmen sind. Obwohl diese notwendigerweise in einer technischen und legalistischen Weise gefasst sind, sind die grundsätzlichen Fragen doch von erheblicher gesellschaftlicher Relevanz. Wie z.B. das gesteigerte öffentliche Interesse und die anhaltende Debatte nach dem Facebook-Cambridge-Analytica-Skandal über die Nutzung und das Sammeln unserer Daten durch Technologiegiganten – sowie das Geschäft in das wir mit diesen Unternehmen eingestiegen sind (Zugang zu „freien" Dienstleistungen im Gegenzug für die Verarbeitung unserer personenbezogenen Daten – welches in Frage 5 thematisiert wird) – zeigt. Ferner wird die Frage, ob Privatpersonen ein Recht auf das Löschen ihrer Daten aus dem *de facto* öffentlichen Register (wie z.B. einer Suchmaschine wie Google) haben, wenn ein entgegenstehendes öffentliches Interesse an diesen Informationen geltend gemacht wird, hitzig debattiert und in diesem Fragebogen unter Frage 8 behandelt.

Die Bestrebung dieses Fragebogens ist es herauszuarbeiten, wie dieses neue datenschutzrechtliche Regelwerk durch die maßgeblichen Vertreter auf nationaler Ebene auf- und angenommen wird (vor allem von Gerichten, nationalen Parlamenten, nationalen Aufsichtsbehörden, und der Zivilgesellschaft). Die gesammelten nationalen Informationen werden dann verwendet, um eine Diskussion über sowohl die datenschutzspezifischen als auch die allgemeinen EU-rechtlichen Fragen, die durch das neue Regelwerk aufgeworfen werden, zu stimulieren.

Der Fragebogen ist entsprechend in vier Kernbereiche unterteilt:

A Setting the Scene – Weichenstellung
B Die Annahme von materiell-rechtlichen DSGVO-Vorschriften in der nationalen Rechtsordnung
C Nationale Durchsetzung von Datenschutzrecht
D Datenverarbeitung für nationale Sicherheitsbelange

A Setting the Scene – Weichenstellung

Die DSGVO eröffnet dem nationalen Gesetzgeber erhebliche Umsetzungs- und Ermessensspielräume durch viele teils äußerst flexible Vorschriften, welches als grundsätzlich eher untypisch bei EU-Verordnungen angesehen werden kann.

1 ***Frage 1:*** *Bitte benennen und erläutern Sie die wichtigsten nationalen Rechtsinstrumente, die eingeführt wurden, um die DSGVO umzusetzen. Gehen Sie insbesondere darauf ein, wie diese Instrumente mit der Flexibilität umgehen, die durch die DSGVO eingeräumt wird (z.B. in Artikel 6 (1) (c); Artikel 23 und 86-90 DSGVO), sowie die Aufsicht, die durch die nationale Aufsichtsbehörde über diese Instrumente ausgeübt wird.*

Die EU-Grundrechtecharta unterscheidet sich von anderen internationalen Menschenrechtsinstrumenten dadurch, dass die Charta spezielle Vorschriften über den Schutz des privaten Lebens und den Datenschutz beinhaltet (nämlich in Artikel 7 und 8 EU-Grundrechtecharta).

2 ***Frage 2:*** *Unterscheidet Ihre Rechtsordnung zwischen diesen beiden Rechten? Hat das Recht auf Datenschutz aus der EU-Grundrechtecharta die Interpretation des nationalen Rechts beeinflusst?*

B Die Annahme von materiell-rechtlichen DSGVO-Vorschriften in der nationalen Rechtsordnung

Obwohl die Leitlinien des EDSA (Europäischer Datenschutzausschuss) eine unterschiedliche Interpretation der materiellen Vorschriften der DSGVO zwischen den Mitgliedsstaaten minimieren sollen, besteht die Möglichkeit, dass die Befunde des EDSA auf nationaler Ebene infrage gestellt werden (beispielsweise durch die Judikative; durch andere Regulierungsbehörden; durch Akademiker; oder, durch Zivilgesellschaft und Medien). Vor diesem Hintergrund werden die nachfolgenden Fragen gestellt.

DSGVO Verantwortlichkeiten

Viele der Schutzmaßnahmen, oder besser der „Grundsätze", des Datenschutzrechts sind seit der Datenschutzrichtlinie von 1995 unverändert geblieben. Trotzdem bleiben die genaue Bedeutung und die praktische Wirkung von wichtigen Grundsätzen in diesem Bereich bis heute ungenau, auch aufgrund nur begrenzter Orientierungshilfe durch die Rechtsprechung des EuGHs.

3 ***Frage 3:*** *Wie haben die für die Verarbeitung Verantwortlichen die Grundsätze der „Verarbeitung nach Treu und Glauben", der Zweckbindung und der Datenminimierung interpretiert und angewendet? Wurden diese Grundsätze von den nationalen Aufsichtsbehörden angewendet und wurden diese durch nationale Gerichte interpretiert?*

Die Artikel-29-Datenschutzgruppe hat eine Stellungnahme bezüglich der Verwendung von „berechtigten Interessen des für die Verarbeitung Verantwortlichen" als Rechtsgrundlage für die Datenverarbeitung und schließlich Leitlinien zum Konzept der Einwilligung (gebilligt durch den EDSA) veröffentlicht.

4 ***Frage 4:*** *Wie wurden diese Rechtsgrundlagen – „Einwilligung" und „berechtigte Interessen" – wohl die wichtigsten und gleichzeitig undurchsichtigsten Grundlagen in der Digitalwirtschaft – durch nationale Gerichte interpretiert?*

Die meisten Dienstleistungen und Inhalte, die im Internet angeboten werden, werden dem Endnutzer frei zugänglich angeboten („free-at-the-point-of-access-to-end-users). Diese Dienstleistungen und Inhalte werden durch das Vorhalten von zielgerichteter Werbung, die genau auf den Nutzer auf Basis seines Onlineverhaltens und der Verarbeitung seiner personenbezogenen Daten abgestimmt ist, finanziert. Somit werden personenbezogene Daten die Gegenleistung oder „Bezahlung" für das Bereitstellen von „kostenlosen" digitalen Inhalten oder Dienstleistungen. Artikel 7 (4) DSGVO legt für Situationen, in denen die Einwilligung genutzt wird um die Verarbeitung von personenbezogenen Daten zu rechtfertigen, fest, dass bei der Bestimmung der Freiwilligkeit der Einwilligung ein besonderes Augenmerk darauf gelegt werden muss, ob der Vertrag von der Verarbeitung nicht relevanter Daten abhängt. Vergleichbar legt Artikel 6 (1) (b) DSGVO fest, dass die Verarbeitung rechtmäßig ist, wenn sie „für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen *erforderlich* [ist]" (eigene Hervorhebung).

5 ***Frage 5:*** *Gab es auf nationaler Ebene eine Debatte oder eine Entscheidung über die Rechtmäßigkeit der Verwendung von personenbezogenen Daten als „Gegenleistung" für die Bereitstellung von digitalen Inhalten?*

DSVGO Rechte

Die DSGVO versucht bereits bestehende Rechte (wie beispielsweise das Auskunftsrecht betroffener Personen) durch eine genauere Bestimmung des Regelungsinhaltes effektiver zu gestalten und führt zugleich ein „brandneues Recht" ein, nämlich das Recht auf Datenübertragbarkeit.

6 ***Frage 6:*** *Artikel 22 DSGVO beinhaltet das Recht nicht „einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden". Artikel 22 (2) (b) DSGVO erlaubt es Mitgliedstaaten gesetzliche Vorschriften zu erlassen um zu bestimmen, dass dieses Recht in gewissen Situationen keine Anwendung findet. Wurden solche gesetzlichen Vorschriften erlassen, und falls ja, welche Vorkehrungen beinhalten diese Vorschriften um die Rechte, Freiheiten und berechtigten Interessen der betroffenen Personen zu schützen?*

7 ***Frage 7:*** *Wie wurde das Recht auf Löschung (Artikel 17), oder dessen Vorgänger aus der Datenschutzrichtlinie (Richtlinie 95/46/EG, Artikel 12), auf nationaler Ebene durch Suchmaschinen, nationale Aufsichtsbehörden oder Gerichte angewendet?*

8 ***Frage 8:*** *Die DSGVO erlaubt es Mitgliedsstaaten gesetzliche Vorschriften zu erlassen, um das Recht auf Datenschutz mit dem Recht auf freie Meinungsäußerung in Einklang zu bringen (Artikel 85 DSGVO). Hat Ihr Mitgliedsstaat ein Gesetz auf Basis von Artikel 85 (2) DSGVO erlassen, und falls ja, wie wurde dieses bisher interpretiert und angewendet?*

C Nationale Durchsetzung von Datenschutzrecht

Die DSGVO revolutioniert die Durchsetzung des Datenschutzrechts in Europa. Einerseits wird durch die DSGVO eine neue EU-Behörde gegründet, nämlich der Europäische Datenschutzausschuss (EDSA) mit der Befugnis maßgebliche Stellungnahmen zu verfassen und, schlussendlich, in bestimmten Fällen sogar bindende Entscheidungen über Angelegenheiten allgemeiner Bedeutung sowie Angelegenheiten die mehr als nur einen Mitgliedsstaat betreffen zu treffen.[1] Andererseits führt die DSGVO eine große Anzahl neuer Rechtsmittel und Strafen, insbesondere hohe Bußgelder sowie die Möglichkeit kollektiven Rechtsschutzes, ein. Das Zusammenspiel dieser neuen Vorschriften mit den bestehenden nationalen Verfahrensregeln wird sich höchstwahrscheinlich kompliziert gestalten. Vor diesem Hintergrund werden die folgenden Fragen gestellt.

Nationale Aufsichtsbehörden sind die Hüter der DSGVO: sie sind mit der Aufgabe betraut die Anwendung der DSGVO zu überwachen und ihrerseits zur einheitlichen Anwendung ebendieser beizutragen.

9 ***Frage 9:*** *Identifizieren Sie die einschlägige öffentliche Behörde (oder die einschlägigen öffentlichen Behörden) in Ihrem Mitgliedsstaat. Skizzieren Sie ihre Zusammensetzung; die Verfahrensregeln für die Benennung von Mitgliedern und Mitarbeitern; jegliche weitere Befugnisse oder Pflichten, die der Aufsichtsbehörde durch nationales Recht*

1 Dieses resultiert aus Artikel 64 (2) in Kombination mit Artikel 65 (1) (c) DSGVO.

auferlegt werden; und, stellen Sie, soweit möglich, die relevanten Details zur „Rechtsdurchsetzungsbilanz" unter der DSGVO zur Verfügung.

Die DSGVO sichert Privatpersonen ein Beschwerderecht bei den Aufsichtsbehörden zu und führt aus, dass die Aufsichtsbehörden den Beschwerdeführer über den Stand und den Ausgang der Beschwerde informieren müssen. Einige Kommentatoren haben befürwortet, dass die Aufsichtsbehörden eine „selective to be effective"-Vorgehensweise (sprich eine selektive Vorgehensweise um größtmögliche Effizienz zu erzielen) bei Beschwerden anwenden sollten, sodass durch diese Priorisierung (z.B. auf Grund von Ausmaß oder rechtlicher Präzedenz) vorhandene Resources gezielt eingesetzt werden können.

10 ***Frage 10:*** *Welche Strategie wird von der Aufsichtsbehörde in Ihrer Rechtsordnung mit Blick auf die Behandlung von Beschwerden verfolgt und, falls einschlägig, welche Einschränkungen werden diesen Strategien durch nationales Recht auferlegt?*

Die DSGVO bietet Mitgliedsstaaten neue Mechanismen um Datenschutzverstöße zu ahnden, welches insbesondere Abhilfebefugnisse (Artikel 58 (2) DSGVO), erweiterte Geldbußen (Artikel 83 DSGVO) und andere Sanktionsmöglichkeiten (Artikel 84 DSGVO) umfasst.

11 ***Frage 11:*** *Wie wurden diese Sanktionsmöglichkeiten durch die Aufsichtsbehörde in Ihrer Rechtsordnung angewendet, und welche weiteren Sanktionen, die über die in der DSGVO explizit vorgesehenen Möglichkeiten hinausgehen, wurden auf nationaler Ebene erlassen?*

Die DSGVO bestimmt, dass betroffene Personen für erlittene materielle und immaterielle Schäden entschädigt werden müssen (Artikel 82 DSGVO).

12 ***Frage 12:*** *Werden in Ihrer Rechtsordnung traditionell immaterielle Schäden kompensiert (in diesem oder in anderen Bereichen)? Falls ja, wie wird ein solcher Schaden genau bestimmt?*

Datenverarbeitungstätigkeiten, besonders im digitalen Bereich, sind durch eine Informations- und Machtasymmetrie zwischen den Datenverarbeitern und den betroffenen Personen gekennzeichnet. Die DSGVO versucht diese Asymmetrie durch das Vorsehen von kollektivem Rechtsschutz in Artikel 80 DSGVO abzumindern.

13 ***Frage 13:*** *Hat Ihr Mitgliedsstaat gesetzliche Regelungen getroffen um diesen kollektiven Rechtsschutz zu vereinfachen? Welche Rolle haben Nichtregierungsorganisationen bei der Datenschutzrechtsdurchsetzung in Ihrem Land gespielt und bilden sich alternative*

Bewegungen auf nationaler Ebene (wie beispielsweise Vereine oder Vereinigungen für personenbezogene Daten) um gegen diese Asymmetrie vorzugehen?

Durch sowohl den wirtschaftlichen Wert als auch den Würdegehalt von personenbezogenen Daten ergibt sich die zunehmende Tendenz, dass andere Regulierungsbehörden, neben den speziellen Datenschutzaufsichtsbehörden, ebenfalls einschreiten (beispielsweise Wettbewerbsbehörden oder Verbraucherschutzbehörden). Außerdem wird in manchen Ländern angedacht neue Regulierungsbehörden für das Internet und für künstliche Intelligenz zu schaffen.

14 ***Frage 14:*** *Sind diese Tendenzen auch in Ihrem Mitgliedsstaat sichtbar? Haben insbesondere die nationalen Aufsichtsbehörden mit anderen Regulierungsbehörden oder Ombudspersonen formell oder informell zusammengearbeitet?*

D Datenverarbeitung für nationale Sicherheitsbelange

Sowohl die DSGVO als auch die JI-Richtlinie schließen die Verarbeitung von personenbezogenen Daten aus Gründen der „nationalen Sicherheit" explizit von ihrem Anwendungsbereich aus. Zum ersten Mal versucht die JI-Richtlinie nunmehr die Datenverarbeitungstätigkeiten von Rechtsdurchsetzungsbehörden zu regulieren. Die genaue Trennlinie zwischen Rechtsdurchsetzungshandlungen, welche vom Anwendungsbereich der Richtlinie umfasst sind, und nationalen Sicherheitsmaßnahmen, die außerhalb dieses Bereichs liegen, kann zu Streit auf nationaler Ebene führen.

15 ***Frage 15:*** *Wird der Begriff „nationale Sicherheit" im nationalen Recht oder in der Verwaltungspraxis Ihrer Rechtsordnung definiert? Haben nationale Behörden die Anwendung der EU-Grundrechtecharta auf die Vorratsdatenspeicherung aus nationalen Sicherheitsgründen akzeptiert (welches sich aus den Urteilen* Tele 2 *und* Watson *ergibt)?*

General Report Topic 2: The New EU Data Protection Regime

Orla Lynskey[*]

General Introduction

The EU first enacted data protection rules in 1995. These rules attracted little attention from EU lawyers for almost two decades. The inclusion of a right to data protection in the Charter of Fundamental Rights of the European Union (hereinafter "Charter") was an early indicator that change was afoot. By the time the EU Commission published its proposals for legislative reform in 2012, data protection was well on its way to a more prominent position amongst EU policy areas. In the intervening period, "data protection" has been catapulted into the spotlight as a result of factors such as technological changes bringing about further datafication, and data-related scandals involving household names such as Facebook.

Thus, the EU's legislative package, comprised of a General Data Protection Regulation[1] (hereinafter "GDPR") and a lesser-discussed Law Enforcement Directive (hereinafter "LED"),[2] which entered into force in May 2018, has generated much debate in scholarly and practitioner communities and, unusually for EU law instruments, amongst the general population.

The design of this questionnaire provided an early opportunity to gauge how the primary and secondary law framework that constitutes "EU data protection law" has been received in domestic legal orders. While there are many aspects of the GDPR that merit critical analysis, the questionnaire focused on those aspects where developments were most likely to occur at national level.

Informing these questions were two background considerations.

---

* Associate Professor of Law, LSE; Visiting Professor, College of Europe (Bruges). With sincere thanks to Katie Nolan, LSE PhD candidate, for her research assistance with questions 2, 3, 4 and 6.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

The first relates to the ostensibly "technical" nature of data protection law. The creation of a new EU body, the EDPB, with the power to issue binding decisions, may give the impression that data protection is a technocratic area of law where clear standards are applied in a manner that is objectively verifiable. However, in reality, the opposite is true. Personal data, and its protection, raises fundamental issues of an economic, social and political nature that cannot be clearly dissociated from the application of the law.

A second consideration relates to the perceived gap between the high level of substantive protection provided for by the data protection framework, in particular the jurisprudence of the Court of Justice of the European Union (hereinafter "CJEU"), and the reality on the ground where data abuses remain prevalent and enforcement action by National Supervisory Authorities (hereinafter "NSAs") appears to be limited.

In order to shed light on these issues, the report sought to assess how Member States had availed of the flexibilities offered by the GDPR (Questionnaire Section A and B) and how they reconciled data protection with other rights and interests (Questionnaire Section B and D). It also probed the changes to the public and private domestic enforcement apparatus brought about by the GDPR (Questionnaire Section C).

The detailed national reports and Institutional Report proved to be treasure troves of qualitative data in drafting this report and merit further reading. In particular, the Institutional Report provides a clear and informative complement to this General Report. Insights from these reports are integrated throughout this report. As they have not yet been paginated, quotes and content are not cited. Where references are made to content contained in national reports, the relevant national report is indicated and the content relates to the question being discussed (unless otherwise specified). Similarly, where references are made to legal provisions (for instance article 23) they refer to the GDPR unless otherwise specified. This report has not sought to complement these reports by conducting additional research into domestic legal systems but rather has attempted to put the domestic developments documented into their broader European context.

1 *Please identify and describe the main national legal instruments that have been introduced to implement the GDPR. In particular, outline how these instruments avail of the most notable flexibilities incorporated in the GDPR (in, for example, article 6(1)(c); article 23 and 86-90 GDPR) and what oversight role the national supervisory authority (NSA) exercises in relation to these instruments.*

Introduction

The GDPR offers considerable routes to flexibility for Member States containing over 50 direct or indirect references to national law. One key theme that emerges from the reports

is that there is significant variation in the extent to which Member States chose to avail of this margin of appreciation, In France, the use of such discretion is "moderate" whereas in Germany the GDPR's opening clauses are used "extensively". In Finland, the aim of the government was to use opening clauses and exemptions to preserve the current legal situation, in particular in the insurance sector and with regard to freedom of speech. Similarly, in the Netherlands an attempt has been made to retain existing national standards and the status quo in order "to enable a smooth transition from the old to the new regime". In Austria and the Czech Republic there was an explicit attempt to prevent "gold-plating" of the GDPR rules by taking maximum advantage of the flexibilities afforded by the regime. As the Czech report notes, the goal was to ensure that the "regulatory burden" on companies was not increased.

While it is not possible to outline exhaustively the ways in which this flexibility has been used, some commonalities across reports are identified.

Article 23 and data protection "restrictions"

Article 23(1) provides that Union or Member State law applying to a data controller may restrict the scope of obligations and rights in article 34, articles 12 to 22 and the corresponding principles in article 5. This restriction should occur "by way of legislative measure", it should respect the essence of fundamental rights and freedoms and it should be a "necessary and proportionate" measure in a democratic society to safeguard one of ten enumerated objectives. These objectives include "public security" and "the protection of the data subject or the rights and freedoms of others". Article 23(2) requires that the legislative measure should contain specific provisions, where relevant, at least as to matters such as the purposes of the processing, the safeguards to prevent abuse and the risks to the rights and freedoms of data subjects.

Implicit in this provision, as the Dutch report notes, is the idea that the right to data protection is not absolute and must be balanced with other rights and interests. Indeed, article 23(1) mirrors the wording – and conditions – of article 52 of the Charter.

The way in which this provision has been received into national law reflects broad differences in approaches between Member States. In some, limitations on specific rights for particular purposes are foreseen in the domestic legislation. For instance, in France there is no right to information if personal data have not been collected directly from the data subject for certain processing relating to the oversight and collection of taxes.

Alternatively, some Member States reproduce the text of article 23 with minor tweaks. This is the case in the Netherlands, where the domestic law is almost identical to the GDPR with one deviation: it does not allow for a restriction of article 5 (the principles relating to

personal data processing) or article 22 (the prohibition on automated decision making, including profiling). Similarly, in the Czech Republic the domestic act allows for the restriction of all the obligations and rights in articles 12-22 and article 5 with regard to all kinds of processing provided the exceptions are necessary and proportionate measures to safeguard the interests listed in article 23(1).

In both the Netherlands and the Czech Republic, the Explanatory Memorandum and Accompanying Act (respectively) indicate that this general provision may be supplemented by sector-specific legislation or more precise rules providing guidance on how the exception applies in concrete cases. The Explanatory Memorandum to the Dutch Act highlights that the provision does not provide a basis for "structural and categorical restrictions of the rights of data subjects" whereas the only safeguard provided for by the Czech Act is that the controller must report every such restriction to the Czech NSA.

The former approach – specifying restrictions to particular rights in specific contexts, as in France – is in line with article 23 and the broader vision of EU fundamental rights it reflects: fundamental rights should be restricted only when necessary and proportionate and respecting their essence. The Dutch approach appears to achieve this same objective through a different means, assuming that "structural and categorical" rights restrictions are not tolerated in practice and that specific legislative measures will provide for required safeguards. However, the Czech approach appears incompatible with the wording of the GDPR, which explicitly requires Member States to introduce restrictions by way of a legislative measure and through article 23(2) to specify further information regarding the restriction. The Czech report notes this tension but justifies the catch-all approach taken as follows:

> It seems practically impossible to *explicitly and specifically* cover all the necessary exceptions for all the possible types of processing in the national law. Moreover, the obligation to report these restrictions to the NSA should pave the way to settled administrative practice and case law with regards to the more common types of processing.

In some Member States it is apparent that the NSA plays a role in scrutinising the way in which the legislature makes use of this discretion. In Ireland, for instance, where ministers make regulations pursuant to article 23, these regulations must undergo a consultation with the NSA. If the minister proceeds with the legislation despite observations to the contrary from the NSA, a written explanation must be provided. Similarly, in Malta the minister responsible for data protection can provide for restrictions pursuant to article 23 provided that the minster for Justice is in agreement and following a consultation with the domestic NSA. It is notable in both these instances that the "legislative measure" introduced is a regulation and that the NSA is consulted but its opinion is not binding.

Flexibility dispersed within the text

Beyond article 23, many other GDPR provisions allow some flexibility for Member States. Two of the most frequently cited examples are set out.

First, a novelty of the GDPR was that it introduced specific legislative provisions applicable to the **processing of children's personal data**. Article 8 sets out specific rules for the consent of a child to the offer of "information society services", providing that:

Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

However, article 8(1) also allows Member States to provide for a lower age limit provided that it is not below 13 years. This provision prompted a necessary discussion on the appropriate balance between the autonomy and privacy of children and their protection.[3] The UK's NSA has, for instance, introduced an age appropriate code of practice for information society services pursuant to a statutory obligation.

There is wide divergence amongst Member States when it comes to the age chosen. It is likely that reports that have not commented on this issue have adhered to the default age of 16. In many of the reports, the minimum age of 13 is noted.[4] The Finnish report, for instance, cites the government proposal claiming that 13 year olds are generally already accustomed to using information society services and that these services are an important platform for self-expression and are also used for schoolwork.

In France an interesting hybrid approach has been adopted. If the child is under the age of 13, consent can only be provided by the person with parental authority (as is required by the GDPR); between 13 and 15 consent must be jointly given by the minor and the person with parental authority; and over 15 the minor can give sole consent. The French government as well as the French *Conseil Constitutionnel* have justified "double consent" based on the wording of article 8(2) which makes a distinction between consent "given" and "authorised" by the holder of parental responsibility. This interpretation could be queried, as the French report notes.

Second, recital 27 states that the GDPR does not apply to the **processing of deceased persons' personal data**. However, it leaves the possibility open for Member States to provide for rules for the processing of deceased persons' personal data. Several Member States have availed of this possibility. In Estonia and Hungary, the national reports indicate

3 M. Stoilova et al, 'Children's data and privacy online: growing up in a digital age' (2019, London: LSE): http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf, all webpages referred to where last visited on 1 February 2020.

4 Belgium; Estonia; Finland; Portugal; Norway. In Greece, 15 is the relevant age.

that specific rules apply or rules apply to a limited extent following the death of a data subject. In Bulgaria, the domestic rules require a legal basis for the processing of personal data of deceased persons. Moreover, controllers are obliged to take appropriate measures to ensure that the rights and freedoms of others or a public interest are not adversely affected. It also provides that the heirs of the deceased person, or other persons with a "legitimate interest" are entitled to get access to the personal data of a deceased person.[5] Pre-existing provisions also exist in Portugal and in France.

Observations

This small insight into how Member States have availed themselves of the flexibilities offered by the GDPR lays bare one of the challenges of data protection regulation in Europe. Although the decision was made to replace a directive with a regulation, this is no ordinary regulation. As we will see below (questions 7 and 8), the reception of these opening clauses into domestic legal orders – their implementation we might say – will lead to significant substantive divergences between the laws of the Member States.

Not only does this challenge the Regulation's ambition for a uniform regulatory environment in Europe, it also makes the domestic legal framework incredibly complex. Many domestic laws combine GDPR provisions with the "implementation" of these opening clauses and the LED. Some, such as Hungary, also include provisions on matters outside the scope of EU law within the same legislation. This convoluted legal landscape challenges the accessibility of the law: the Czech report notes that "the Act itself is somewhat difficult to understand for the common citizen", the Italian law involves "difficulties of interpretation" while the French law is described as "difficult to read bordering on unintelligible".

2 *Does your national legal order differentiate between these rights? Has the EU Charter right to data protection influenced the interpretation of national law?*

Introduction

The Charter is distinct amongst international instruments being the first to incorporate distinct provisions relating to the right to respect for private life and the right to data protection (articles 7 and 8 Charter). Moreover, as the Institutional Report notes, the CJEU

5 E. Harbinja, 'Post-mortem privacy 2.0: theory, law and technology', *International Review of Law, Computers and Technology*, Vol. 31, No. 1, 2017, p. 26.

has invoked these provisions to dramatic effect to declare several Union instruments invalid and provide a negative opinion on a draft international agreement.

Distinct rights: in search of a common constitutional tradition?

Despite the separation of data protection from the right to respect for private life in the Charter, a significant number of Member States either do not acknowledge data protection as a right at all (for instance, Bulgaria and Slovakia) or, if they do, they treat is as a subset of the right to privacy.[6] Yet a similar number of States have in their constitutional frameworks a distinct right to the protection of personal data alongside protection of the right to privacy.[7] These Member States can be distinguished in the following ways.

Contrasting specific and general approaches

Some countries prescribe very specific protections, while others express the right in more general terms. In Poland the right is framed in quite specific terms. The Polish Constitution explicitly establishes the right to data protection. Thus, article 51(1) provides that "No one may be obliged, except on the basis of statute, to disclose information concerning his person". Article 51(2) controls the use of information by public authorities, prohibiting them to "acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law".

In Germany, by contrast, there is a constitutionally protected general personality right "which ensures for the individual a right to a protected space for free development". Alongside this right, there is also a judicially created right to data protection.

The Czech Republic protects a free-standing right in its domestic Charter. Article 10(3) of the domestic Charter explicitly provides for protection against unauthorised collection, publication or other misuse of personal data. This appears to be a halfway house approach: it is more specific than article 8 of the European Convention on Human Rights (hereinafter "ECHR") but less detailed than the Charter. Yet, as the report notes in domestic jurisprudence, it is this right that is referenced rather than international alternatives, and it is viewed as a sort of semi-independent right to informational self-determination.

Established versus modern rights

Portugal has the distinction of being the first written constitution in the world to recognise the protection of personal data as a fundamental right, including this right amongst its

6 In particular, such an approach is seen in Belgium, Estonia, Finland, France, Malta, the Netherlands and Switzerland.

7 Namely, Austria, Croatia, the Czech Republic, Germany, Greece, Hungary, Poland, Portugal, Slovenia and Spain.

provisions since its approval in 1976. The original article was entitled "Use of computerised data". It provided for a set of fundamental rights related to data processing through automated means that was intended to ensure informational self-determination. Interestingly, this constitutional provision was amended in 1997 to adjust to European secondary legislation, the Data Protection Directive (hereinafter "DPD"), by extending its material scope to the processing of personal data other than by automated means.

Spain and Austria have both recognised the right to personal data since 1978. In Austria, a fundamental right to data protection was introduced in 1978 and exists alongside article 8 ECHR, which has constitutional status in Austria. The Austrian Constitution also protects other more specific communications privacy rights such as the Secrecy of Correspondence (article 10) and Telecommunications secrecy (article 11).

In Spain, the Constitution of 1978 explicitly acknowledged the protection of personal data within the privacy right. However, the Spanish Constitutional Court clarified the distinct nature of the right to data protection in a landmark ruling of 2000 that confirmed its autonomous character. Hungary is also amongst the Member States that was an "early adopter" of the right to data protection, enshrining this right in its Constitution for the first time in 1989.

These long-standing rights can be contrasted with more recent additions to national constitutional landscapes. In Croatia, a distinct constitutional right to data protection was introduced by amendment in 1997. Article 37, guaranteeing the "safety and secrecy of personal data", provides that, in the absence of consent, processing may only be done under conditions specific for law. Article 37 also provides for a strict form of purpose limitation, requiring: "The use of personal data contrary to the express purpose of their collection shall be prohibited".

In Greece, explicit protection for personal data was introduced in 2001 under article 9A of the Constitution. Article 9 protects the right to private and family life, while the article 9A specifically protects the right to protection of personal data. Separate, constitutionally independent administrative authorities are responsible for the protection of the differentiated legal rights conferred by articles 9 and 9A. Article 9A, which belongs to the new generation of "e-rights", focuses on electronic data processing, but also covers non-automated, conventional processing by traditional means.

Reliance on the Charter

The Spanish report notes that, even prior to the Charter acquiring binding status in 2009, the Spanish Constitutional Court had relied on it, and other international texts, when confirming the autonomous character of the right to data protection. It is therefore

interesting to consider what, if any, impact the Charter rights have had at national level over the following two decades later.

A number of Member States have not yet seen any explicit reliance on the Charter.[8] Some insights into why this is the case can be gleaned from the reports. In Bulgaria the Charter continues to be viewed as an "exotic instrument" compared to the ECHR while in Austria the Charter is perceived as having no additional value on top of existing constitutional protection. Norway's particular status as a European Free Trade Association (hereinafter "EFTA") state to which the Charter does not apply has meant these rights have not yet had any influence, however an indirect interpretative effect based on the incorporation of CJEU Charter case law by Norwegian courts and authorities is not ruled out.

However, in the majority of Member States, the Charter and the judgments of the CJEU interpreting articles 7 and 8 have had some, often considerable, impact.[9] Even in Member States where there was a pre-existing right to data protection, such as the Czech Republic and Portugal, the Charter has been regularly invoked. In particular, the Charter rights have been used as a benchmark to assess the legality of domestic legislative provisions. For instance, in Slovenia the Charter has been invoked alongside domestic constitutional provisions to declare a provision of the Protection of Documents and Archives Act unconstitutional. The Constitutional Court decided that submission and retention of materials of psychiatric institutions containing sensitive personal data on psychiatric treatment to a public archive to make this material available to the public implies an interference with the patients' constitutional rights to the protection of personal data, privacy and the inviolability of personal dignity. In so finding, the Constitutional Court referred to articles 7 and 8 of the Charter and the CJEU's *Schecke* and *Eifert* decision.[10]

Interestingly, NSAs have also referred to the Charter in their decisions and deliberations. In Poland, the "independence" of NSAs referred to in article 8(3) Charter, as well as relevant CJEU jurisprudence (such as *Commission v Hungary*[11]), was the subject of discussions during the work on provisions to regulate aspects of the NSA's functioning. Even more notable is a decision of the Luxembourg NSA that considered the "essence" of the right to data protection. The decision concerned a legislative bill that proposed introducing restrictions to certain GDPR rights in the fiscal field on the basis of article 23(2). The aim of this legislative bill was to restrict the scope of these rights in a proportionate way so as not to hinder tax collection by the administration through direct contributions. The NSA noted in its opinion that the limitations adopted must respect the essence of the right to

8 Austria; Bulgaria; Denmark; Germany; Hungary.

9 Finland; France; Ireland; Poland; Portugal; Slovenia.

10 Judgment of 9 November 2010 in Joined Cases C-92/09 and 93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662.

11 Judgement of 8 April 2004 in Case C-288/12, *European Commission v Hungary,* ECLI:EU:C:2014:237.

data protection. However, according to the NSA, the legislative bill nullified the essence of the right to data protection by limiting the rights guaranteed by the GDPR in their entirety.

Elucidating the meaning of these rights

It is clear that the Charter rights to privacy and data protection, and the CJEU jurisprudence interpreting them, have been playing an important role at national level. Some Member States nevertheless continue to treat data protection and privacy as synonymous despite their separate enumeration in the Charter. The Belgian Constitutional Court, for instance, considers that the Charter rights are "analogous in scope to article 8 ECHR". Indeed, the distinction between the two rights has not yet been clearly elucidated by the CJEU in its jurisprudence, as hinted at by the German report, which suggests that the interpretation of article 8 "raises questions of its own".

There has been much doctrinal debate about this question, with many important issues remaining unresolved.[12] Some of this is reflected in the national reports. The Spanish Constitutional Court considers the rights to be distinct in their scope, with the right to data protection being wider than the right to respect for private life as it protects data in the public domain. Moreover, it considers that data protection gives individuals "a group of positive powers to control personal information". The ultimate objective of this broad reach and enhanced control is hinted at in the Luxembourg report, which notes that the Charter right to data protection has inspired a proposal to include a right to informational self-determination and data protection in the Constitution. As the report notes, the principle of informational self-determination based on the values of human dignity and autonomy is recognised in the academic literature to have an inextricable link with data protection. However, as it also notes, the consequences of anchoring this right at constitutional level remain unclear. The same can be said, for the moment, about the anchoring of a right to data protection at primary law level in the EU.

3 *How have data controllers interpreted and applied the principles of "fair" processing, purpose limitation and "data minimisation"? Has the NSA applied these principles and have they been interpreted by domestic courts?*

12 G. González Fuster & H. Hijmans, 'The EU right to privacy and personal data protection: 20 years in 10 questions', VUB Working Paper, 13 May 2019: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_González_Fuster_Hijmans.pdf.

Introduction

The principles of "fair" processing, purpose limitation and data minimisation constitute core data protection principles that are common to many data protection frameworks worldwide[13] and formed a key pillar of EU data protection law in the 1995 Directive. Nevertheless, despite their centrality to the data protection regime, there has been little jurisprudence to inform the application of these principles. Moreover, the (former) Article 29 Working Party, an advisory body comprised of representatives of domestic NSAs, provided guidance only on the concept of purpose limitation. The principle of fairness, in particular, is enigmatic from a legal perspective and has only in recent years attracted the attention of academics, primarily, yet not exclusively, in the context of automated decision making where there is a growing "fair, transparent and accountable" machine-learning community.[14]

It is therefore surprising, yet reassuring, to note from the national reports that while judicial findings regarding these principles remain rare, a rich decisional practice from NSAs applying these principles exists, some aspects of which will be highlighted.

Before doing so, it is worth noting that in transposing the 1995 Directive some Member States failed to directly incorporate some principles at national level. In Slovenia, we are told that the former data protection law did not directly include a data minimisation principle, albeit that the report suggests that domestic courts tried to plug this gap. In Germany, a principle of "data economy" was in place rather than data minimisation. Similarly, as discussed below, in many Member States the principle of fairness was not directly incorporated into national law. In Poland, the controller's obligation is expressed to be one of "due diligence" (although the Polish translation of the Directive referred to fairness). The Polish report suggests however that in practice this duty of "due diligence" in processing data served as a synonym for "fairness". What will be interesting to consider is how in the future these pre-existing – and distinct – domestic concepts will affect the interpretation of the GDPR principles at national level.

Data minimisation

The principle of data minimisation provides that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are to be

13 L.A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford, Oxford University Press, 2014, chapter 5.

14 See, for instance, J. Ausloos & D. Clifford: 'Data Protection and the Role of Fairness', *Yearbook of European Law*, Vol. 37, 2018, p. 130.

processed".[15] What emerges from the reports about this principle are examples of assessments arising in the context of complaints or queries regarding the extent of data collection necessary for certain purposes. The reports reflect a fact-based assessment of compliance with data minimisation, taking into consideration the purpose for which the data is being processed.

Several examples arise in the context of employee data processing by employers. In Italy, the NSA used its power to ban data processing in the context of employee-related data through the use of vehicle tracking systems. In Croatia, the NSA was asked to consider whether it is lawful for employers to send employee biographies to potential clients in Croatia and abroad. The NSA concluded that the data that can be included in such a transfer must be limited to information relating strictly to the professional experience and knowledge of employees.

The processing of employee personal data (including gender, sexual orientation and ethnicity) to prevent workplace discrimination for promotions, salaries and other was deemed by the NSA to be incompatible with data protection law in Sweden. This was upheld on appeal with the court finding that the information gathered would not constitute a large enough dataset to serve its stated purposes. As a result, this led to the unnecessary storage of highly personal information. Further, the court considered the information collected to be too wide relative to the stated purpose and that the need to store the data in the long term clashed with storage minimisation.

The processing of national identification data in inappropriate circumstances has also led to a number of notable decisions. For example, in Hungary a recent, post-GDPR decision of the NSA reviewed the check-in requirements for a festival. The festival collected the personal data of festival-goers during mandatory security screenings by making copies of IDs and taking photos at the entry gate. The NSA found that the scope of data processed (including citizenship, number and ID expiration dates, date of birth and gender) was excessive in relation to the purpose of the processing. The retention period of one year was also deemed excessive.

The Czech Constitutional Court also recently annulled part of the law that required the tax identification number (corresponding with the national identification number) of the seller or service provider to be stated on every receipt.

It is interesting to note that data minimisation does not entitle the data subject to specify specific data security or data minimisation measures, according to the Austrian NSA. Thus, there is no right to have data pseudonymised for instance.

15 Art. 5(1)(c) GDPR.

Purpose Limitation

Purpose limitation means that data is be collected for specified, explicit and legitimate purposes and not processed further in a manner incompatible with those purposes.[16] Processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes is deemed to be compatible.[17] Guidance on how the "compatibility" element of this principle is to be interpreted when the processing is not based on consent or compliance with a legal requirement is found in article 6(4).

Sometimes a breach of this principle is evident. For instance, the Eastern High Court of Denmark held that the purpose limitation principle was violated when a real estate agent used his access to a credit information system to obtain and pass on information about a local politician's unpaid debt. Equally, in Belgium the use of personal data obtained from a neighbourhood watch WhatsApp group to send personal election materials was deemed to infringe purpose limitation.

In the majority of cases however a more context-specific assessment is required. The Danish NSA considered a case concerning an insurance company that sought access to recordings and observations from inside the policyholder's home when the policyholder made a claim. The NSA held that the use of such recordings may be justified in order to fulfil the stated purposes however in this situation there was no information on whether the policyholder's activities within the home were relevant to the case. In the Czech Republic, a complaint was raised about companies using publicly available registers, such as the land register, for advertising purposes. The NSA decided that not all the data from such registers can be fully used for marketing and commercial purposes without the consent of the data subject.

The Norwegian Supreme Court has arrived at the obvious yet important finding that the existence of a legal basis, in situ legitimate interests, does not relieve the controller of the obligation to comply with all data processing principles, including purpose limitation. In the case before it, a driver who had been dismissed because of discrepancies between his time sheets and the electronic (GPS) log of his vehicle requested damages for non-economic loss pursuant to data protection law. The Supreme Court's majority concluded that reusing information collected for a purpose other than the original one cannot be justified on the basis of legitimate interests of the controller alone. Rather, the principle of purpose limitation must also be satisfied. In that case, the employer's comparison of the log and the time sheets represented a reuse that was incompatible with the original purpose of data collection. The Court held that the data processing was unlawful, even though the legitimate interest test was apparently satisfied.

16 Art. 5(1)(b) GDPR.
17 Ibid.

The various visions of fairness

The principle of fairness can be difficult to articulate. While "fairness" is a well-established benchmark in consumer protection law,[18] resort to this concept in other areas of law has been more controversial.[19] A primary point of contention is whether the concept is so nebulous or subjective as to impede legal certainty. Nevertheless, the reports provide ample evidence of the application of this concept at national level. The Slovenian report, for instance, notes that the most frequent infringement investigated in recent years has been the violation of this principle.

Looking at the examples provided, it is clear however that what is considered unfair differs across jurisdictions and regulators.

An early judgment handed down by the Hungarian Constitutional Court linked fairness to the purposes of data processing, finding that personal data may only be processed for a definite and legally-justified purpose and that every stage of the processing must conform to this.

The Swiss and Austrian reports link the principle of **good faith** to the notion of fairness. In Austria the principle of fairness is violated if a controller has a policy that entailed the deletion of all personal data, even in situations in which the data subject requested partial deletion.

Discriminatory practices in Finland were held to be unfair by the Finnish NSA. It held that the way a credit information company was establishing credit scores was discriminatory as a very low or high age would cause an application for credit to be automatically inadmissible.

According to the Hungarian courts, the principle of fairness is **broader than lawfulness.** The courts were asked to adjudicate on an appeal against an NSA decision finding that a liquidation company had violated principles of purpose limitation and data minimisation. The liquidation company had processed the data of third parties beyond the debtor, including the data of neighbours and family members of the debtor, and a wider set of data than necessary, including data on the medical condition, family life, work status and tax identification numbers of data subjects. The court considered that the principle of fair processing is a broader requirement for data processing than the principle of lawfulness. The court also deemed the processing of third-party data to be unfair as it created an

18 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council [2005] OJ L149/22 and Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ("Unfair Commercial Practices Directive") [2006] OJ L364/1.

19 See, for example, A. Jones et al, *EU Competition law: Text, Cases and Materials*, Oxford, Oxford University Press, 2019, p. 31.

asymmetry between the data controller and the data subject whereby the data subject was not in a position to be aware of what the data controller knew about them. The Hungarian Supreme Court upheld these findings.

In the UK, fairness has been linked to the reasonable expectation of the data subject in NSA guidance:

In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

A decision of the NSA provides an insight into how this might be applied in practice. The NSA investigated data processing by a pregnancy and parenting club, which collected personal information for the purpose of membership registration through its website and mobile app, merchandise pack claim cards and directly from new mothers at hospital bedsides. The company also operated as a data broker service, supplying data to almost 40 third parties including credit reference and marketing agencies. In its decision, the NSA indicated that the controller failed to use the personal data of the 14 million affected data subjects fairly. In particular, data subjects "registering with a pregnancy and parenting club would not reasonably have expected their personal data to be disclosed to the likes of credit reference, marketing and profiling agencies". The Austrian NSA similarly reasoned that the filming of people in traffic using a dash cam breached the principle of fairness as it was not reasonable to expect that they would be filmed, in particular in situations not involving accidents.

However, the dominant application of the fairness principle connects fairness to the transparency principle. This is perhaps unsurprising given that article 5(1)(a) provides that personal data shall be processed "lawfully, fairly and in a transparent manner". Indeed, both the Czech and Greek reports indicate that the NSAs consider these three principles together as an inseparable combination. The reports provide good examples of the ways in which this link between transparency and fairness is made. In Ireland, for example, the correct use of CCTV has arisen in many previous NSA case studies. In one case study, a bus operator discovered one of its drivers using a mobile phone when driving while reviewing CCTV footage in the context of a customer complaint. The driver later complained about the use of this footage against him in a disciplinary procedure. The operator was found to have contravened the fairness principle by failing to properly or fully inform staff that CCTV footage may be used in disciplinary proceedings. A Belgian court has held that the lack of sufficient information about Facebook's systematic tracking of internet users on third-party websites (irrespective of whether they were Facebook users) violated the principle of fair processing.

Which of these visions of fairness will be endorsed by the CJEU remains to be seen. The Irish report also hints at another development that may be of significance in the coming

years: "There remains a concern that while an organisation could be compliant with the principles of GDPR, they must also ensure that they process personal data 'fairly'". This suggests that fairness could be an over-arching responsibility beyond legal compliance and could be linked to current debates about the role of ethics in technology regulation. Equally however it could be understood as indicating that, within the GDPR, fairness operates as a stand-alone principle with its interpretation being independent of other principles (for instance, transparency). This, it is suggested, is the preferred approach yet it is clear that more elucidation of "fairness" is required to promote legal certainty.

4 *How have these legal bases – "consent" and "legitimate interests" – arguably the most significant yet opaque in the digital environment – been interpreted by national courts?*

Introduction

The CJEU's *Planet49* judgment affirmed how valid "consent" should be interpreted, in particular the requirements that consent should be "specific", "unambiguous" and "informed".[20] According to the Institutional Report, the ruling "suggests that informing users that, by continuing their activity on a website ('continuous browsing') they consent to the placing of cookies on their devices is not sufficient for consent to be valid". Yet, such commercial practices remain commonplace, indicating that there is widespread disregard for the law. Moreover, from the perspective of individuals, "consent" might be viewed as a legal fiction, "partly overloaded in light of the realities of the digital economy" as the German report notes.

The primary alternative legal basis to consent available to private parties is "legitimate interests". The Article 29 Working Party provided guidance on how this legal basis, now found in article 6(1)(f), should be interpreted. Given the potential significance of this legal basis should consent be applied as required by the CJEU, it is useful to also consider its application domestically.

Legitimate interests

Many Member States reported that their local NSAs and courts had provided guidance on the nature of the legitimate interests legal basis. We consider these below according to two themes: findings which turned on whether a given interest could correctly be deemed "legitimate", and those which focused on the balancing of competing interests and rights that this provision entails.

20 Judgment of 1 October 2019 in Case C-673/17 *Planet49 GmbH*, ECLI:EU:C:2019:801.

A *Interrogating the meaning of "legitimate interest"*

The reports provide some informative examples of interests that have not met the "legitimate" threshold, including the following:

- The checking of bank account activity to exercise disciplinary control on employees (Greece) or the use of personal data to measure performance in the workplace (Sweden).
- The interest of local authorities to register detailed statistics of the contents of the garbage of individuals (Sweden).
- The compilation of statistics on how the healthcare system operates (Sweden).

The reports also provide examples of interests deemed to be legitimate by NSAs and domestic courts. For example, in Ireland the Supreme Court considered the provision of fingerprints to UK authorities by the Irish Refugee Appeals Commissioner to comprise a legitimate interest as it served the purpose of obtaining information relevant to the task of determining the Member State responsible for dealing with the relevant refugees' applications under the Dublin regime.

An interesting approach is taken in Spain where the national law specifying elements of the GDPR includes a number of rebuttable presumptions that a certain interest should be deemed legitimate if the regulation's requirements are met. These include the processing or use of an individual's contact details when they are acting as entrepreneurs or professionals (article 19), processing for credit information systems (article 20) and some commercial operations (article 21).

B *Balancing exercise*

We see many examples of NSAs and courts grappling with the balancing of legitimate interests against competing interests of the data subjects. The CJEU has provided guidance on how this balance should be struck in *Rigas Satiksme*[21] in which it set out three cumulative conditions that must be taken into consideration. First, the interest pursued must be legitimate. Second, the personal data processed must be necessary. Third, there must be an overall balancing of rights and interests. The Czech Supreme Administrative Court has emphasised this final balancing of rights and interests in one of its judgments. It considered the necessity and proportionality of the use of CCTV in order to achieve its stated aim before stating that the importance and gravity of the two fundamental rights opposing each other must be assessed in the light of the factual circumstances of the case at hand

21 Judgment of the Court of 4 May 2017 in Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme"*, ECLI:EU:C:2017:336.

(balancing *stricto sensu*). This approach can be contrasted with Slovenia where the legitimate interest must be evident and not require a detailed or in-depth balancing exercise.

In Estonia, the Supreme Court has indicated that it is not relevant when assessing legitimate interests whether the data processing, in fact, helped to achieve the interest pursued. That case concerned the wrongful dismissal of a public official who had experienced workplace bullying. To prove that she was being bullied, she recorded a conversation without asking the permission of the official whom she was recording. The Court held that it was irrelevant whether the recording had helped to achieve the legitimate interest when striking this balance, as it was not possible to know this at the time the recording was undertaken. What was important was that the personal data processing had been to achieve the legitimate interest and that the plaintiff only disclosed the recordings to the relevant authority. The Court also held that the controller's interest must be a lawful one and that the need for processing should be real and not just hypothetical. It ultimately concluded that the plaintiff had the overriding legitimate interest to get evidence of the alleged bullying in the workplace in order to demand that it cease.

Consent

Unsurprisingly, many Member States reported that their NSAs or courts had considered complaints or questions in relation to consent. Four notable themes emerge: the prevalence of consent as the default legal basis for processing; the practice of obtaining consent online or in relation to digital services; consent in the workplace; and the attention paid to whether consent was freely given (considered in the next question).

A Consent as the primary norm

Consent is viewed as the primary norm, or default legal basis, for personal data processing in a number of Member States, most notably in those Member States where there is a strong tradition of informational self-determination.

In the Czech Republic, the Supreme Administrative Court has held that the right not to have personal data processed without consent is part of the right to informational self-determination protected by the Czech constitution, article 8 ECHR and, more broadly, a part of one's integrity as a fundamental precondition to a dignified existence. The domestic legislation implementing the DPD treated consent as the "principal legal basis" for any processing of personal data; other legal bases were merely an exception. According to the Czech report, despite the changes introduced in response to the GDPR "the aim and purpose of the consent of the data subject remains" and the Supreme Administrative Court itself noted in one particular case that the GDPR "would not change its conclusions".

Similarly, in Germany, consent and contract are examined as a priority as legal bases for data processing with legitimate interests construed narrowly by supervisory authorities. Consent is said to put the power in the hands of the data subject while legitimate interests shifts this power to the data controller. For instance, in March 2019 the German Data Protection Conference (the Conference of Commissioners) stated in an opinion that, in principle, consent for tracking measures is required and legitimate interests can only be relied upon in exceptional cases.

B Obtaining consent online or digitally

Some reports drew attention to NSA decisions regarding how consent was sought or obtained for digital services.

In Spain, for example, the NSA determined that the app offered by the Professional Football League failed to comply with the GDPR consent requirements, specifically in relation to the system for the activation of the microphone and the location of the device.

The UK NSA considered a complaint regarding 289,790 unsolicited e-mail communications sent to existing contacts to clarify their marketing preferences. The controller was unable to show that the recipients had consented to receiving the messages. The NSA determined that the verification messages themselves constituted marketing based on the UK legislation which implements the e-Privacy Directive.

Actions have also been taken against prominent technology companies for consent violations.

For instance, in 2018, a Belgian court ordered Facebook to stop tracking Belgian internet users, whether generated through Facebook or third-party domains via certain types of cookies and similar technologies such as pixels, without their consent. A cookie banner warning internet users that Facebook places cookies on the basis of further browsing was not considered sufficient in this regard because, amongst other things, (i) users were not sufficiently informed about the systematic placement of cookies without further use or about the essential elements of such processing (such as the nature of the data collected through cookies); (ii) users without a Facebook account could only express their lack of consent by leaving the Facebook homepage, which entails negative consequences for the user; and (iii) a user could only consent to all cookies and could not make a granular choice.

C Consent in the workplace

A number of Member States noted that enforcement actions had considered the capacity for consent to be obtained from existing or potential employees.

The Austrian NSA held that, although consent is possible in the employment context, it has to deliver a clearly recognisable advantage to the employee. In 2011, the Danish Supreme Court stated that unspecified consent from a potential new employer to collect references from a former employer could not cover the collection of highly sensitive personal data, for instance regarding potential alcohol abuse. More recently, in 2016, the Hungarian NSA issued guidelines on the basic requirements of data processing in the context of employment, where it noted that consent can only be valid in the employment context in exceptional situations given the relationship of subordination between employer and employee.

As shall be discussed presently, the question of whether consent can be considered freely given when services are offered on a take-it-or-leave-it basis, has been hotly debated in the context of services that are free at the point of access where data may be considered as the quid pro quo for the service.

5 *Has there been debate or a decision at national level regarding the validity of personal data as counter-performance for the provision of digital content?*

Data protection law is not applied in a vacuum. As Zuboff documented in *Surveillance Capitalism*, current business models embed and shape economic incentives that encourage ever-more personal data processing.[22] This dynamic is implicitly referenced in some reports. The Finnish report, for instance, notes that Finnish media companies do not collect the same amount of personal data for personalisation as international social media companies. However, the Swiss report notes that the major Swiss media houses and the public media company announced in 2019 that they would collectively introduce registration for all online content from September 2020 onwards. This was justified on the basis that "the media houses will receive additional data from their users, which will enable more targeted advertising". The report suggests that publishers want to strengthen their competitive position vis-à-vis the big US technology companies.

However, this business model raises questions about the fairness of the exchange for individuals. As the Luxembourg report notes, it is questionable whether in the context of digital services there is a real freedom of choice when access to digital content is made conditional on data processing. Moreover, even if consent is deemed to be freely given, should we question whether "too much" data are extracted in such circumstances, or should the law impose any limitations on this market transaction?

We see from the national reports that in some jurisdictions such issues have been given almost no consideration at all, or consideration only within academia. This is the case in Denmark, Poland and Portugal. Yet, in other Member States this issue has been given

22 S. Zuboff, *The Age of Surveillance Capitalism,* London, Profile, 2019.

considerable attention. In Italy, the Italian Competition Authority (AGCM), the Communications Regulatory Authority (AGCom) and the Data Protection Authority jointly launched a "Big Data fact-finding survey", which considered this issue amongst others.

A matter of contract law

The Maltese report acknowledges the lack of jurisprudence on this issue in Malta. The report opines that personal data could be viewed as "lawful consideration" for the purposes of the Maltese Civil Code and that the validity of a contract based on personal data processing would be upheld by a court of law. The UK report suggests that the lack of debate on this topic in the UK may be attributable to the "common law's traditional *laissez-faire* attitude to the freedom to contract".

Thus, this issue can be looked at as an issue of domestic contract law. From this perspective, both the Hungarian report and the Norwegian report suggest that local legal experts criticised the Draft Guidelines of the European Data Protection Board (hereinafter "EDPB") on data processing under article 6(1)(b) in the context of the provision of online services (the draft guidelines).[23] The essence of this critique is that the EDPB overextends its authority by straying beyond questions of GDPR into issues of contract law which is "clearly and firmly within the domain of national courts". Novovic, co-author of the Norwegian report, asserts that by "making sweeping statements on the 'general purpose of the contract' for the entire categories of online services, and consequently engaging in contract interpretation, EDPB is seriously overstepping its authority and the scope of tasks conferred on it by the virtue of article 70 of the GDPR." In Hungary, the claim is made that the underlying conceptions of the GDPR are being applied to "fundamentally different" processing activities from those the GDPR was meant to regulate, and that data protection is being treated as "some kind of super law, the principles/regulations of which should be given more weight than the regulation of other areas of law".

In Italy, in contrast, such transactions are not looked at as a matter of contract law. The joint report (alluded to above) considers that the business relationship is "implicit" not contractual as there is no "economic compensation, since the market, missing a regulatory framework on the trade of data, does not assign any price to the transaction".

Counter-performance through the lens of consumer protection law

In Luxembourg the consumer code provides that describing a product as "free", "without cost", "free of charge" or in a similar way is considered to be an abusive commercial practice if the consumer must pay other costs related to the commercial practice. The Luxembourg

23 European Data Protection Board, Guidelines 2/2019 on the processing of personal data under art. 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019.

report notes that it could take inspiration from France where the "Unfair Terms Commission" held that "free" clauses led the consumer or non-professional to believe that the service does not require any other counter-performance on its behalf although the data, information and content provided when using social networks constitutes a kind of counter-performance that may have a value to professionals.

As the UK report notes, the most serious debate on this subject was conducted within the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament before the adoption of EU Directive 2019/770 on contracts for the supply of digital content and digital services in May 2019.[24] This Directive must be transposed by July 2021 and will apply from January 2022. The Greek report indicates that the discussions concerning this directive since 2015 and the broader discussions regarding a "New Deal for Consumers" proposed by the European Commission in April 2018 have spurred this debate at national level. The latter, as the Irish report notes, seeks to extend consumer protection rights to "free" digital services in which personal data is processed in lieu of payment.

In the Netherlands both Chambers of the Dutch parliament addressed questions to the government in 2018 regarding the lack of clear coordination between the Digital Content Directive and the GDPR. However, the negotiation of this legislative instrument culminated in explicit references to the GDPR. Therefore, the final text of the Digital Content Directive provides that it applies where a trader provides digital content or services to consumers in exchange for personal data, except where such personal data are exclusively processed for the purpose of supplying the content or services or for compliance with a legal obligation and the trader does not process the personal data for any other purpose.[25] Article 3(8) of the Directive specifies that EU data protection law applies to the processing of such data and that, in the event of any conflict between the Directive and data protection law, the latter should prevail.[26]

A matter of data protection law

What then does data protection law have to say about this issue? In its Guidelines, the EDPB indicates in the online behavioural advertising context that the article 6(1)(b) legal basis – where the processing is necessary to enter into or perform a contract – cannot be relied upon simply because advertising indirectly funds the provision of the service. It notes that:

24 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

25 Ibid, art. 3(1) Digital Content Directive.

26 Ibid, recital 37.

> "Although such processing may support the delivery of a service, it is separate from the objective purpose of the contract between the user and the service provider, and therefore not necessary for the performance of the contract at issue."

If such processing cannot be justified on the basis that it is *necessary* for contractual purposes, attention then turns to a likely alternative legal basis: consent. In order for consent to be valid it must be freely given, specific and informed. Article 7(4) states that when considering whether consent is freely given:

> "[U]tmost account shall be taken of whether […] the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

There are two elements of this provision that are of particular interest: first, the performance of the contract is conditional on consent (conditionality, or bundling) and, second, the processing must be necessary for the performance of the contract (necessity).

Necessity

Article 7(4) is an inherently circular provision as it requires analysis to revert to the question of whether the processing is indeed necessary for the performance of the contract. There has been some national divergence of how "necessary" should be interpreted in this context. In Slovenia, the Information Commissioner, in the context of its opinion on the Digital Content Directive, noted that there was a risk that such contract would be used to legitimise situations where an individual actively provided more personal data than would be reasonably necessary to perform the contract. Similarly in Austria there has been discussion about the impact on consent if the benefit granted in return for consent is of little value. The report predicts that the NSA and courts will make strict demands on the "free" nature of consent in this respect.

In Italy, the Supreme Court has determined that a website that provides fungible services can legitimately subject the provision of the service to the condition that the processing of data for advertising purposes, provided that the consent is individually given and linked to the specific purpose. Implicitly this judgment would therefore seem to accept that advertising was "necessary" for the performance of the contract.

This can be contrasted with a finding of the Austrian Supreme Court that held, in the context of a collective action against a TV service provider regarding clauses in its general terms and conditions that, if the conclusion of the contract is made conditional on consent to processing of personal data that is independent of the contract, it cannot be assumed that the consent is freely given. The Supreme Court considered that such a strict

interpretation of when consent is freely given can be derived from articles 4(11), 7(4) and recital 43 GDPR.

Further facts regarding these judgments are not provided. However, what seemingly differentiates the two is that, in the first, the data processing itself indirectly subsidised the content through advertising revenue and was thus deemed necessary, whereas in the latter it is possible that the TV service provider imposed a fee on customers and yet made its service contingent on unnecessary data processing.

Conditionality or bundling

Equally controversial is the question of whether, or to what extent, the provision of a service or content can be made conditional on providing consent to data processing. The answer to this question will hinge on how article 7(4) is interpreted by the CJEU. As the Institutional Report notes, in *Planet49* the Advocate General referred to the "selling" of personal data in his Opinion, in the sense of "agreeing to be contacted by so-called [online lottery] sponsors for promotional offers",[27] however this issue was avoided by the Court.

The German report indicates that a strict ban on so-called consent bundling "may most likely not be derived" from article 7(4). One factor that seems to be playing an important role is whether there are alternatives available to the data subject.

In a much-discussed decision, the Austrian NSA has considered the withholding of a service in the absence of consent to be lawful if persons affected had a choice and could receive the same service through a paid option that did not entail personal data processing. In that case, an online newspaper presented affected individuals with the option of either purchasing a paid subscription for €6 per month or accessing the content free of charge but granting consent to the use of cookies for advertising purposes. The NSA concluded that such consent could be given freely, since the absence of consent would not cause any major disadvantage given that, amongst other things, the online subscription was not excessively expensive, and other newspapers provided news and the content could be accessed in print form.

A further differentiating feature is whether "conditionality" relates only to the provision of a primary service (for instance retail services) or also related secondary services (such as loyalty programmes and discount opportunities).

The Czech NSA issued a decision regarding the loyalty programme of the national railway company that offered customers a loyalty programme with discounts if they consented to data processing for marketing purposes. In its decision, the NSA stated that membership of the loyalty programme was entirely voluntary and that the services of the controller (primarily train travel) can be accessed without being a programme member.

27 Opinion of AG Szpunar of 21 March 2019 in Case C-673/17 *Planet49 GmbH*, ECLI:EU:C:2019:246, para. 99.

The NSA indicated that the special prices and offers provided to loyalty programme members are entirely within the controller's discretion, which can therefore decide under which conditions it will offer benefits to customers.

The latter can be contrasted with a decision of the Belgian NSA, which considered that consent to the processing of the data subject's national e-Identification in exchange for the use of a loyalty card was not free. In particular, the NSA held that consent "cannot be regarded as freely given if there are no alternatives available to the customer to benefit from discounts." Thus, while in the Czech case the NSA considered conditionality in relation only to the primary service – which could still be accessed in the absence of data processing – the Belgian decision considers that conditionality also applies to "optional" services where the primary service remains available irrespective of the data processing.

When considering these decisions, it is difficult to separate the assessment of the "free" nature of the consent from economic considerations, in particular whether the processing subsidises the service and whether there are economically viable alternatives available. Yet, whether such interpretations are compatible with the fundamental rights underpinnings of data protection law remains contested. In France, the influential civil society organisation *La Quadrature du Net* advocated for the exclusion of personal data from the Digital Content Directive on the basis that it could not be viewed as a commodity. Critics of the Austrian decision claim that the presence of a paid alternative does not necessarily result in "free" consent and that the impact of this "pay or okay" approach needs to be considered cumulatively. The risk, according to such critics, is that data protection becomes a luxury item, available only to those who can afford to pay for content that is not subsidised via personal data processing rather than an inalienable right.

On the other hand, there are those who suggest that viewing data as counter-performance for the provision of a contract simply acknowledges the current economic reality. The Norwegian report, in particular, identifies some of the key arguments against the EDPB's recommendation that "personal data cannot be a tradable commodity". It suggests that the GDPR does not address personal data commodification directly and that it is for the legislature or the judiciary to resolve any disputes. It also notes that the Charter protects "freedom of contract", a fact which should have been given a central place in the Guidelines.

What is certain is that the EDPB is correct in stating that while data subjects can agree to the processing of their personal data, they cannot trade away their fundamental rights. Short of such a waiver of rights, the precise terms of the exchange between data controllers and data subjects is likely to receive considerable attention – and likely varying appraisals – across EU States in the coming years.

6 *Article 22 provides for a right not to be subject to automated decision making, including profiling. Article 22(2)(b) allows Member States to introduce legislative measures to*

ensure this right does not apply in certain situations. Have such legislative measures been introduced and, if so, what measures to safeguard the rights, freedoms and legitimate interests of data subjects do they incorporate?

Contextual background

Article 22, and its predecessor article 15 DPD, reflect one of the first attempts globally to regulate the use of automated decision making (hereinafter "ADM") and to introduce "due process" protections for such decisions.[28] According to the EDPB, article 22 should be read as a prohibition rather than a right that must be invoked by data subjects.[29] It provides that:

> "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[30]

This prohibition does not however apply if the data subject explicitly consents, if the processing is necessary to enter into or perform a contract or if authorised by Union or Member State law. Thus, article 22(2)(b) affords Member States the possibility of allowing for this ADM, even if it affects individuals. However, it also specifies that this law must lay down "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". Article 22(3) sets out a similar requirement where the decision making is based on consent or contract but stipulates that it should include "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". It remains to be determined whether these particular minimum safeguards also apply when ADM is made permissible by law.

The GDPR thus embeds the perspective that ADM requires additional legal safeguards for individuals when compared to non-automated decision making. Some of the key concerns voiced in the vast literature on this concern the transparency, contestability and accountability of such decision making.[31]

The reports reflect some distinct attitudes to the risks of such processing. The Dutch government has, for instance, held firm in the face of industry calls (from the Dutch Trade

28 D. Keats Citron & F.A. Pasquale, 'The Scored Society: Due Process for Automated Predictions', *Washington Law Review*, Vol. 89, No. 1, 2014, p. 1-34.

29 EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6 February 2018.

30 Art. 22(1) GDPR.

31 For a systematic overview of concerns see, Mittelstadt et al, 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society*, Vol. 3, 2016, p. 1-21.

Association) to create more generous exemptions to article 22 in order to facilitate more "options for innovation regarding new profiling-based techniques". In a letter to the House of Representatives in April 2019, the government noted, in particular, the risk that group characteristics are attributed to an individual while it is not 100% certain that this individual, although belonging to the group, shares these characteristics. This cautious approach is also reflected in its initiative to establish a working group to create guidelines for, amongst other things, the transparency of algorithms used by the government.

A less cautious approach is visible in other reports. Most notably, the Bulgarian report indicates that the national legislator has permitted the automated processing of special categories of personal data (such as data on ethnicity, racial origin, religious or political affiliations) provided suitable safeguards are in place. Article 22(4) maintains that special categories of data should only be used for ADM when based on consent or in the public interest and accompanied by suitable safeguards. The Bulgarian provision appears to be incompatible with this requirement as the claim could not be made that *all* ADM serves the public interest.

A No Implementation

There are several States where no legislative measures have been introduced to apply the option of "no implementation" offered by article 22(2)(b). These include Croatia, Estonia, Greece, Luxembourg, Malta, Portugal, Norway and Switzerland.

In Norway a legislative initiative applicable to public administration is currently being debated that would facilitate further digitalisation of administrative activities. According to the Law Commission, it envisages the full automation of administrative proceedings, subject to a requirement "that the legal content of the system must be publicly documented". Similarly, in Switzerland the precise circumstances of and conditions for the use of ADM are still being debated at this point.

B Implementation on a broad or general basis

In the UK and in Sweden, we see a broad approach to the application of article 22(2)(b), allowing for the possibility of a wide range of permitted ADM. For example, in the UK, the domestic data protection act provides that where a controller takes a "qualifying significant decision" in relation to a data subject based solely on automated processing:

a. the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and
b. the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to:

i. reconsider the decision; or
ii. take a new decision that is not based solely on automated processing.

The NSA has provided further guidance on this section, taking the view that:

If you have a statutory or common law power to do something, and automated decision making/profiling is the most appropriate way to achieve your purpose, then you may be able to justify this type of processing as authorised by law. However, you must be able to show that it's reasonable to do so in all the circumstances.

C *Implementation by specific or limited exception*

Many Member States have exercised their discretion by introducing specific or limited exceptions to the prohibition on ADM in article 22(2)(b).

For example, in Poland, a series of amendments were made to specific sectoral laws to ensure that the prohibition on ADM does not apply in certain situations. These include the Banking Law; Road Transport Law; the Insurance and Reinsurance Activities Law and the National Tax Administration Law, to name but a few. The legal measures enacted specify exhaustive categories of personal data which can be used in ADM. Similar style provisions exist in Denmark and in Germany for insurance purposes.

Some references to the specific safeguards introduced by States are evident. In the Netherlands, exemptions to the prohibition are available if ADM does not pose a high risk of having a discriminatory effect. Therefore, ADM for "closed" decisions that are "based on the fulfilment of objective requirements", are thought not to be high risk. Some examples include processing income data for tax purposes or basing traffic fines on photographs in combination with licence plates.

In Hungary, a provision of the Hungarian Code of General Administrative Procedure, pre-dating the GDPR, allows automated decision making if:

a. it is permitted by an Act or government decree;
b. all data are available to the authority at the time of the submission of the application;
c. decision making does not require deliberation; and
d. there is no party with opposing interests.

D Recognition of prohibition in domestic law

Some laws affirm the prohibition in article 22 explicitly via law. For instance, in the Czech Republic it is generally forbidden to issue "true administrative decisions" based purely on automatic decision making.

Although not explicitly banned, it follows from the French implementing law that machine learning algorithms (which develop a model based on training data and make predictions and inferences without being programmed to do so) cannot be used as an exclusive basis for administrative decisions. There has also been a long-standing rule in French law (dating from 1978) that no judicial decision involving an assessment of the behaviour of a person can be made algorithmically.

Observations

In many domestic legal systems, the GDPR is the only legal framework applicable to ADM. Yet, as these examples illustrate, the protection offered by article 22 is quite precarious. Even if the conditions of article 22(1) apply in principle, Member States can introduce legislative provisions circumventing this prohibition. ADM may be desirable if specific safeguards are in place to protect individuals. However, some scepticism is required if this circumvention occurs by relying on broadly framed exceptions. Moreover, the safeguards offered by the GDPR in this context appear to be highly individualised – the right for an individual to express their point of view and to contest the decision – raising the question of whether these safeguards can be harnessed by groups who are systemically affected by ADM.[32]

7 *How has the right to erasure (article 17), or its Data Protection Directive predecessor (Directive 95/46 EC, article 12) been applied at national level by search engines, the NSA or Courts?*

Context

Article 17 sets out a right to erasure ("right to be forgotten"). Pursuant to article 17(1) data subjects have the right to have the controller erase personal data concerning them without undue delay if one of a number of grounds enumerated in the provision applies. These include situations where the personal data are no longer necessary in relation to the

32 See, L. Taylor et al (Eds), *Group Privacy: the Challenges of New Data Technologies*, Dordrecht, Springer, 2017.

purposes for which they were collected or otherwise processed[33] and where the personal data have been unlawfully processed.[34] However, this right is not absolute as it may be limited pursuant to article 17(3), amongst other things, for the protection of freedom of expression and information.

The previous formulation of the right of erasure in article 12(b) DPD arguably achieved the same objective yet in simpler terms. It provided that Member States must guarantee the data subject the right to obtain from the controller, as appropriate:

> the rectification, erasure or blocking of data the *processing of which does not comply with the provisions of this Directive*, in particular because of the incomplete or inaccurate nature of the data. (Emphasis added)

This provision is perhaps most known for its application by the CJEU in the 2014 *Google Spain* judgment.[35] Since then, there have been almost 895,000 requests to delete data relating to over 3.5 million URLs, 53.8% of which have been declined.[36] Some Member States, for instance Austria, report that the right to erasure was one of the key topics in complaint procedures following the entry into force of the GDPR.

In the Netherlands, the percentage of URLs that were delisted jumped from 47.8% to 56.3% following the entry into force of the GDPR. The national report suggests this change may be attributed to the strong awareness campaign run by the NSA and the government in the run up to this date. Similarly, in Spain – where the NSA acted as a pioneer for the "right to be forgotten" – adopting its first Resolution on the right in 2007 – a considerable volume of jurisprudence around the right has been developed.

This can however be contrasted with many other Member States where the right is ostensibly yet to be embedded in domestic legal orders. There has been no case law or decisional practice on this right in Denmark, and very limited activity in other jurisdictions such as Luxembourg, Estonia, Norway and even Germany (where the national report suggests the right to erasure has been relied on much less frequently than the right to information).

Interest in this right and its application has therefore varied across Member States. However, as this right requires a reconciliation of data protection and privacy interests with freedom of expression and information interests, even where it is applied there will be substantive variation across Member States. Indeed, the Irish report notes that although

33 Art. 17(1)(a) GDPR.

34 Art. 17(1)(d) GDPR.

35 Judgment of 13 May 2014, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

36 Google Transparency Report, requests to delete relating to 3, 515, 080 URLs, https://transparencyreport.google.com/eu-privacy/overview (data accurate as of 24 February 2020).

approximately 25% of all cross-border processing complaints received by the NSA in 2018 related to erasure, a large proportion of these cases were dealt with locally by the "home" NSA. As the report notes, erasure requests generally "involve an assessment of a single data subject request in the context of local, on-the-ground conditions" and this transfer of competence is facilitated by article 56(2).

The CJEU has since acknowledged this national divergence in *Google LCC,* cited in the Institutional Report. The Court has suggested that the GDPR consistency mechanism will be sufficient to enable NSAs to find a common solution to eventual discrepancies.[37]

In terms of terminology, it is clear the term "right to be forgotten" is often used to describe the de-indexing of content from search engines with the right to erasure being a broader term. However, neither the text of the DPD nor the GDPR makes such a distinction. Moreover, the article 17(2) obligation on controllers to whom an erasure request has been addressed to take reasonable steps to inform subsequent controllers of this request to discourage further dissemination is sometimes also referred to as a "right to be forgotten".

Normative foundations for the right

The Spanish report provides some insights into the normative foundations of this right. The jurisprudence of the Spanish Constitutional Court treats it as a "defence mechanism that an individual has to protect her honour vis-à-vis informational initiatives or mistakes that may endanger the moral integrity or reputation of the interested person". As the Italian report notes, requests to delete or update information processed lawfully arise due to the passage of time or changes to the source of the information. As such, the right is intended to be a "dynamic projection of the right of the person not to remain indefinitely exposed to further damages their reputation may suffer due to the repeated publication of news legitimately disclosed in the past".

Furthermore, the Spanish report notes that rectification (as opposed to erasure) may help to guarantee free public opinion by establishing the veracity of information in the public sphere. For instance, the Spanish Act provides that when addressing requests for rectification, digital media should publish an explanatory notice in their digital archives indicating that the original notice does not reflect the current situation of the individual. This notice must be in a visible place alongside the original information.

Factors influencing erasure requests

A number of elements relevant to establishing a deletion claim emerge from the national reports.

37 Judgment of 24 September 2019 in Case C-507/17, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772, para. 67-69.

First, it may be relevant to consider whether the controller has a countervailing right or obligation not to delete the data. This issue has been addressed in several Swedish court cases. For instance, the Supreme Administrative Court has found that where publicly accessible documents containing personal data must be archived, the data cannot be erased. This may also be the case in relation to court records. For instance, the Maltese report notes that there has been considerable controversy surrounding the decision to allow the request for erasure of certain online criminal court judgments from the public record. Such requests are made directly to the court registrar who is the data controller for the court. It seems that, in the majority of such cases, the judgments were being anonymised rather than removed from the record (112 of 176 requests for removal of judgments from the public domain culminated in anonymisation, while 41 of these were rejected outright).

A second relevant factor is data accuracy.[38] The principle of data accuracy requires that personal data must be up to date. Moreover, the GDPR states that "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."[39] The more time that passes, the greater the likelihood that information may become out of date. Conversely, in Italy, the Court of Lucca has held that the right to be forgotten should be excluded if a short interval has elapsed between the facts on which a case is based and the case itself. Such a short interval is "undeniably insufficient to weaken the collective interest in knowledge and dissemination" of the information.

In Ireland, the High Court considered the application of the data accuracy principle in a case involving a request from a local politician to have a Reddit chat forum criticising his campaign and labelling him as homophobic delisted from Google's search results. The High Court considered that a lower court had erred by considering the accuracy only of the heading of the text and held that in assessing accuracy it should have considered the entirety of the text of the discussion.

A third factor is the viability of alternative rights, such as rectification. In France a court has upheld a finding that an individual whose personal data were erroneously processed under the American Foreign Account Tax Compliance Act (hereinafter "FACTA") had the right to the total erasure of these data. In particular, the Court held that the relevant bank could not limit itself to a rectification of the error. The data subject had the fundamental right, according to the court, to have all their data definitively erased from the file held pursuant to FACTA.

38 Art. 5(1)(d) GDPR.
39 Ibid.

Rights of primary publishers

In *Google Spain*, the CJEU distinguished between distinct data controllers in the context of the provision of internet search engine (ISE) results. In particular, it noted that the primary publishers of content indexed on ISE could be distinguished from the ISEs. In the UK, in *NT1 and NT2* the Court took account of this distinction and acknowledged that the original news source (newspaper articles) could benefit from the exemption for journalistic purposes (discussed further in Q8) while ISE could not. As a result, the rights of the data subject will apply differently to distinct data controllers.

This is recognised in Polish jurisprudence, which incorporates the ECHR and indicates that it is not a violation of an individual's article 8 ECHR right when a court refuses to order a newspaper to remove articles from an internet archive that damage an individual's reputation. Domestic courts consider that the internet constitutes a form of press and the task of the press is to describe events that are currently taking place, even if circumstances subsequently change. As such, there are no grounds for published articles to be monitored by the publisher or journalist for their accuracy.

In Belgium, the Court of Cassation has taken a more nuanced approach. While the Court recognised the right of publishers to put digital archives online and for the public to access these archives, it held that such rights are not absolute. In this case, an individual who was criminally convicted for involvement in a traffic accident in 1994 had a contemporaneous news report republished in a digital archive in 2008. The Court held that the online archive was a new disclosure of the claimant's criminal history, which violates his right to be forgotten. The Court confirmed the decision of the lower court to award compensation for moral damage (of €1) and to anonymise the article. The Court of Cassation issued a similar judgment in November 2018.

In Hungary, a domestic court refused to allow an individual – a lawyer whose father had been accused of serious criminal offences and whose name and profession were referred to indirectly in newspaper articles – to exercise his right of erasure vis-à-vis the newspaper. The Court considered that the *Google Spain* reasoning was only of relevance in relation to search engines and not a newspaper, even if it operated a search function within its website.

Google Search has a practice of informing primary publishers when their content is de-indexed in certain circumstances in response to a deletion request. *Google Spain* had not taken into account the "interest of the newspaper itself in having wider accessibility of its website", as the Institutional Report highlights. Implicit in this practice is recognition of this fact. Nevertheless, the Spanish NSA imposed a fine of 150,000 euro on Google for

this practice in 2016. A Spanish court later declared this fine void in April 2019, despite serious reservations that this practice is incompatible with EU data protection law.[40]

Observations and future developments

From the outset, the dereferencing facilitated by the right to erasure has led to questions about whether and how the rights to data protection and privacy can be reconciled with freedom of expression. The CJEU has begun to unpick this balancing exercise in its jurisprudence. In *Google LLC* it has held that NSAs and judicial authorities remain competent to balance the data subject's rights with freedom of expression in light of national fundamental rights standards and, where appropriate, to order the dereferencing of content on all global domain names. However, this approach raises more questions than it answers, as astutely observed by the Institutional rapporteurs:

> "The precise implications of this consideration are unclear. How the national balancing exercise can be separated from the European one, keeping in mind that both will relate to the same request for delisting is unclear. It is equally unclear what value should be given to the considerations of the Court that numerous *third States* do not recognise the right to deferencing or have a different approach to it and that the outcome of the balancing exercise is likely to vary significantly around the world."

8 *The GDPR allows Member States to legislate to reconcile the right to data protection with freedom of expression (article 85). Has your state introduced a law pursuant to article 85(2) GDPR and, if so, how has this been interpreted and applied to date?*

Introduction

Article 85 provides for a general reconciliation of freedom of expression and data protection.

Article 85(1) GDPR requires Member States to reconcile by law, "the right to freedom of expression and information, including 'processing for journalistic purposes and the purposes of academic, artistic or literary expression'". Article 85(2) indicates the specific chapters of the data protection framework from which derogations may be permitted for these purposes, in essence all but the provisions on judicial remedies, liability and sanctions.

40 D. Erdos, 'Communicating Responsibilities: The Spanish DPA targets Google's notification practices when delisting personal information', Inforrm blog, 21 March 2017, www.inforrm.org/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/.

This provision is interesting as it is broader in its framing than its predecessor (article 9, DPD). The latter enabled Member States to introduce exemptions or derogations to specific chapters to the extent necessary to reconcile data protection and privacy if processing is carried out solely for journalistic purposes or for the purpose of artistic and literary expression. Article 85 GDPR is broader in a number of senses: it enables a general reconciliation of freedom of expression and data protection, including but not limited to processing for journalistic, academic, artistic and literary purposes; processing no longer needs to be *solely* for journalistic purposes; and it now explicitly incorporates processing for academic purposes. It is thus instructive to consider whether Member States have adapted their approach to this reconciliation in order to avail themselves of this increased latitude.

The need for reconciliation by law

The GDPR requires that the reconciliation of data protection and freedom of expression is by law. Despite this requirement, in Norway and Estonia no such laws exist to date while in Portugal the provision referring to the balance between these rights does not provide for limits or specific guarantees beyond those in the Constitution.

Several Member States have sought to reconcile the two rights within the text of the domestic data protection legislation. This is the case in Bulgaria, Greece, Ireland, the Netherlands and the UK, for instance. Some of these provisions are very broadly framed. The Irish legislation, for instance, exempts personal data processing for freedom of expression purposes where "compliance with the provision would be incompatible with such purposes". As a safeguard, the domestic legislation enables the NSA to refer the case to the High Court to seek a determination on any question of law relating to whether a specific processing operation is exempt from compliance with a GDPR provision on freedom of expression grounds. The Austrian report raises the prospect that such vague provisions are incompatible with EU law as it delegates the required balancing to the instance applying the provision instead of providing for this balancing in law.

"Journalistic activity" and the public interest

The notion of processing for "journalistic" purposes has been carried over from the 1995 Directive. As documented in the Institutional Report, the CJEU has had the opportunity to expand upon its meaning on a number of occasions. Most recently, in *Buivids* the Court built on its previous finding that activities are "journalistic" when they disclose to the public information, opinions or ideas, irrespective of the medium in which they are transmitted. In particular, the Court held that uploading a video to YouTube could be

considered processing for solely journalistic purposes only if its sole objective was to disclose information, opinions or ideas in this way.[41] It clearly follows, for instance, that not all personal data published on the internet benefits from this exception. In Sweden, there is extensive court practice on the interpretation and limits of "journalistic purposes". Consistent with the jurisprudence of the CJEU, it has been held that, if information aims to inform, criticise and create debate on current issues of interest to the public, such publications pursue journalistic purposes.

Such an approach differs starkly from the wording of the Austrian legislation, which indicates that processing is for journalistic purposes only if it is done for the purposes of "the media company or media service". The Austrian NSA has however interpreted this provision in line with relevant CJEU case law to incorporate "citizen journalism".

Several reports suggest that whether the personal data processing is in the public interest is a significant factor in balancing data protection and freedom of expression. For instance, in Bulgaria a significant recent NSA opinion regarding the publication by the Prosecutor's Office of press releases and information for journalists relating to accused persons in the pre-trial context, the NSA considered such processing lawful if there is an "overriding public interest". As a general rule the personal data of others should not be published in the pre-trial context unless, again, there is an overriding public interest. The NSA notes an exception to this, namely data relating to persons holding high public positions (as defined by statute) which "by its nature has an effect on the public".

Yet, Member States differ in what they consider to be in the public interest. In Denmark the NSA held in its "Black Register" decision that a webpage run by "Black Register" featuring the name, job title and work phone number of public servants under headings such as "abuse of power" and "neglect of duty" was lawful. This webpage also sometimes included the date of birth and political affiliations of civil servants. The NSA reasoned that the webpage was part of a public debate and enabled opinions to be voiced.

In Slovenia, media rights are limited when it comes to processing personal data and case law distinguishes between "ordinary citizens'" and "public figures", and within the latter category between "absolute" and "relative" public figures. The degree to which the individual enters into public life leads to a proportionate reduction in the privacy they enjoy. Absolute public figures are those who are constantly under the scrutiny of the public due to their role and function in society (for instance, politicians, entertainers and other artists, top athletes, officials, etc.). Relative public figures are those persons who are of interest to the public only temporarily because of their connection with a particular event (for instance, winners of various competitions or events, perpetrators of serious crimes and others). Publishing information on relative public figures is only permitted if it is of

41 Judgment of 14 February 2019 in Case C-345/17, *Sergejs Buivids*, ECLI:EU:C:2019:122, para. 69.

interest to the public due to the event and not later. Therefore, whether the "Black Register" case would have been decided in the same way in Slovenia is doubtful.

Contested ground: evidence of contestation at national level

Striking the appropriate balance between data protection and freedom of expression is one of the most contentious aspects of data protection legislation. That contestation over the appropriate balance between these rights is occurring at national level is evident from the reports.

This disagreement is, for instance, arguably reflected in the limited (arguably unlawful) reception of article 85 in some Member States. The French legal framework focuses on processing for journalistic purposes to the exclusion of the other forms of processing (artistic, academic and literary) mentioned in article 85(1) GDPR. In Austria, processing for journalistic purposes is treated in a separate provision to processing for these alternative purposes, and it benefits from a blanket exemption from the GDPR requirements. In this sense, it does not incorporate the required "necessity" element of article 85(1). Nor does the Danish implementation, where journalistic purposes and journalistic databases are exempted in their entirety from the scope of the domestic act. In the Czech Republic, the Czech parliament introduced general exceptions for processing for the purposes specified in article 85(1) indicating its scepticism regarding the more nuanced approach – with specific exceptions – proposed by the government.

More explicitly, in the Netherlands the government stated openly in a letter to the House of Representatives that it would not be following the recommendation of the news companies' trade organisation to exempt news companies from more GDPR provisions. In Bulgaria, a request signed by fifty members of parliament is pending before the Constitutional Court asking it to find that the domestic reconciliation of right is contrary to the national constitution and the ECHR. The European Law Association contests this claim.

Future developments

The CJEU has been cautious in giving substantive guidance on how these rights should be reconciled. Moreover, as the national reports reflect, the scope for divergence in this area is significant and, it could be added, the EU lacks the competence to harmonise freedom of expression directly. The GDPR foresees that Member States must notify the Commission of the provisions adopted to reconcile these rights and of any subsequent amendments without delay. In this regard, the conclusion reached by the Institutional Report is justified:

> "Even more than under the previous *Directive*, the Commission will feel compelled to search for a certain coherence in this area in order not to undermine the harmonising effect of the present *Regulation.*"

9 *Identify the relevant public authority (or authorities) in your Member State. Outline its composition; the appointment process for members and staff; any additional power or duties the NSA is entrusted with under national law; and, provide relevant details regarding its 'enforcement record' under the GDPR.*

Introduction

One of the significant innovations of the GDPR was its attempt to strengthen and Europeanise the enforcement mechanisms for data protection.[42] Nevertheless, Member States are left with significant latitude in designing the bodies tasked with enforcing the rules, NSAs, subject to the proviso that these NSAs are independent as required by article 8(3) Charter and article 16 of the Treaty on the Functioning of the European Union (hereinafter "TFEU"). It is evident from the national reports that States have taken advantage of this discretion as there is a wide range of NSA profiles and procedures on display.

Composition

Article 51(1) requires each Member State to provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR, to protect the fundamental rights and freedoms of individuals and to facilitate the free flow of data within the Union. The domestic legal status of these supervisory authorities is very varied, for instance the UK NSA is a "corporation sole" while the Dutch NSA is an autonomous administrative authority endowed with legal personality. In Germany data protection authorities are present at Federal and at *Länder* level and work together in the "data protection conference".

Most of the NSAs are comprised of a president or commissioner and some deputies along with their staff. The French NSA – the CNIL – is the most unusual in its composition. The CNIL is composed of a multidisciplinary college of 18 members of which 9 are appointed by political organs (parliament or government).

---

42 O. Lynskey, 'The "Europeanisation" of EU data protection Law', *Cambridge Yearbook of European Legal Studies*, Vol. 19, 2017, pp. 252-268.

A common, and perhaps surprising, feature that emerges from the reports is the creation of various forms of advisory boards and expert groups at national level, which provide the NSAs with non-binding guidance. In Finland, the NSA is supported by an Expert Board comprised of five members. The role of the Expert Board is to give non-binding opinions upon a request by the Ombudsman on high-profile issues relating to the application of data protection legislation. In Belgium, the NSA is supported by an independent Reflection Council, consisting of representatives of the business world, professional federations, consumer organisations and the academic world. There is a similar body – a Council – in Spain and it is provided for by Polish law.

The staffing levels across NSAs also vary drastically. The Estonian NSA, for instance, currently employs 17 staff and has seen no major increase since the introduction of the GDPR. Many of the other NSAs employ somewhere between 30 and 80 people with some significant outliers. Cases in point are the Hungarian NSA which employs 114 people and the CNIL which employs 215 people. The UK NSA is however by far the most significantly staffed as it currently employs just under 700 people. This number was increased from just over 500 following the entry into force of the GDPR "with particular increases in the parts of the organisation handling data protection complaints and customer contact". Some NSAs have also engaged in internal restructuring to arrange their workload. The Danish NSA consists, for instance, of a council and a secretariat: the former decides in leading cases, while the Secretariat handles day-to-day cases and matters.

The independence of NSAs

Article 52 GDPR is dedicated to ensuring the independence of NSAs. This provision incorporates the findings of the CJEU's jurisprudence relating to the concept of independence. For instance, the NSAs must be free from external influence, whether direct or indirect, and must neither seek nor take instructions from anybody.[43] It also specifies various conditions for independence including budgetary independence, for instance.

Some national reports raise the issue of independence. According to the German report, German constitutional law generally requires that authorities engaged in administrative actions should be subject to supervision in order to guarantee their democratic legitimacy. Indeed, the German Federal Government had raised this constitutional issue in its defence during infringement proceedings brought by the Commission, which (successfully) claimed that this supervision of the NSA was incompatible with its independence under EU law.[44] Moreover, this report notes that there are other practical possibilities for influence over

43 Art. 52(1) GDPR.

44 Judgment of the Court of 9 March 2010, Case C-518/07, Commission v Germany, ECLI:EU:C:2010:125, para. 25.

the domestic supervisory authorities as is evident in Germany. For instance, the report queries whether the supervision from supervisory authorities provided for by some state constitutions is compatible with independence.

In other reports, independence is not explicitly mentioned but some of the conditions regulating the NSA may give rise to concerns. In Bulgaria, for instance, although the NSA has its own income, it also obtains part of its income from the fines it imposes if they are upheld by the court. This possibility again may give the impression that the NSAs fines could be motivated by financial considerations.

Enforcement record

Comparing the NSAs' enforcement records thus far is a difficult task given that there is no uniform metric for recording systems deployed across NSAs (or evident from these reports). Therefore, some of the NSAs record their activity in terms of the number of complaints received while others document the number of procedures commenced or completed. Nevertheless, despite this difficulty in comparing data, it is notable that several reports provide evidence that the relevant domestic NSA has seen a significant increase in demand for its services since the GDPR's entry into force. The UK NSA's annual report for 2018-19 refers to the year as "unprecedented". Its helpline, live chat and written advice services, for instance, experienced a 66% increase in contacts compared to the previous year. There was also a significant increase in the number of complaints received: this shifted from 21,019 in the 2017-18 period to 41,661 in the 2018-19 period.

The UK NSA was not alone in experiencing such a surge in demand. In Luxembourg the NSA received double the number of written requests for information in 2018 than in 2017, with the number of complaints received also doubling from 200 in 2017 to 450 in 2018. In Croatia the number of complaints lodged with the NSA rose by 260%. Similar dynamics were indicated in France and Denmark (where the NSA expects three to four times more cases under the GDPR than previously). In the UK and Luxembourg it is noted that the majority of these complaints relate to the right of access to personal data (38% and 24% of complaints respectively).

The Portuguese report sensibly highlights that, in addition to this increased domestic activity, the consistency mechanism brings a further line of work to the NSAs, one that is having a real impact on the enforcement activity at national level.

One question this surge in demand raises is how NSAs are coping with it. We shall consider this now.

10 *What strategy for complaint handling is taken by your NSA and what, if any, constraints does domestic law place on such a strategy?*

Introduction

Article 77 provides data subjects with the right to lodge a complaint with an NSA and states that the NSA must inform the complainant of the progress and outcome of the complaint including the possibility of judicial review. In particular, article 78(2) provides that the data subject will have the right to an effective judicial remedy if the NSA does not "handle the complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged".

In dealing with the significant increase in workload post-GDPR, Member States have approached this task in different ways. In Spain, the NSA has sought to enhance prevention of data protection violations, as part of its Strategic Plan 2015-19, in order to ensure more effective data protection. It has therefore engaged in various targeted information and media campaigns, paying special attention to minors and education. Luxembourg has managed this shift primarily by increasing the workforce of the department dealing with complaints to allow all to be addressed. According to the Norwegian report, the Norwegian NSA is ostensibly dealing with this issue in part by discouraging data subjects from submitting complaints. The NSA website instructs data subjects to submit written rather than electronic complaints and urges data subjects to resolve their issues directly with data controllers. The Swedish NSA similarly emphasises the importance for individuals to try to resolve potential problems themselves while in Greece the individual must appeal to the controller, or Data Protection Officer if one has been appointed, before submitting a complaint to the NSA. The Czech Republic inverts the process: the NSA is required by legislation to have a yearly inspection schedule. With its remaining resources, the NSA responds to individual complaints and queries.

One issue that this increase in regulatory activity raises is whether the NSA can adopt a "selective" approach to the complaints it receives. Article 58(1)(f) provides that NSAs must handle complaints lodged by a data subject or a relevant body "and investigate, to the extent appropriate, the subject matter of the complaint". The meaning of the "to the extent appropriate" in this context is ambiguous.

Indeed, what is surprising is how few Member States require all complaints to be investigated to a certain extent. This is the case in Austria, Finland, Malta and Portugal. The Austrian report states that a selective strategy would be inconsistent with Austrian administrative procedural law, which bars the NSA from making a selection amongst the initiated proceedings before it. The Portuguese report also explicitly states that the NSA has no margin of discretion on this issue and that it cannot "ignore complaints based on an assessment of minor pertinence".

The reports indicate that implicitly or explicitly a selective approach to complaint handling or enforcement is being taken at domestic level.

In Norway, an implicit enforcement prioritisation seems to be at play. The Norwegian report notes that almost all enforcement action thus far has stemmed from breaches of article 32 and that there is a "clear focus on data security as an enforcement mechanism trigger". As the report also suggests however, this strategy may be flawed in the long term if it encourages data controllers to envisage their data protection obligations in an unduly narrow manner. In Denmark, there is no published strategy for dealing with complaints; however the report notes that the volume of cases is forcing the regulator to "be very selective when deciding what cases to pursue or not".

Many of the reports highlight the conditions for admissibility of complaints. These include whether the subject matter of a complaint has already been reviewed by a court or administrative authority (Slovakia); whether the complaint is submitted abusively (such as if the complaint is a repeated one; Greece); or if there are court proceedings pending (Hungary). Anonymous complaints are also rejected in some Member States (Greece and Hungary, for example).

Strategic selectivity

These admissibility conditions may also directly or indirectly consider the strategic significance of a complaint. The Hungarian NSA rejects complaints relating to minor infringements while, in Sweden, whether an alleged infringement is a systematic or recurrent breach is taken into consideration when assessing admissibility. Indeed, there is considerable evidence of "strategic selectivity" in the reports. In Belgium, for example, the NSA can decide at every stage of the complaint procedure whether to dismiss the case with a view to an effective and efficient enforcement policy.

The UK's enforcement responsibilities are said to be "intelligence led" according to the NSA. This means that information received from various sources is used "to inform a strategic threat assessment, which will support all of our work, including investigations, enforcement, guidance, codes of practice and more".

Similarly, the Italian Code differentiates between complaints and "reports". The latter may be anonymous and are directed to solicit oversight of an area rather than concrete individual violations. The NSA does not need to adopt a measure based on a report however if it deems it necessary, it can start a control if it "sees the risk of serious prejudice or retaliation to the detriment of subjects concerned by the treatment, or for cases of particular gravity".

In Ireland, given the status of the NSA as "lead authority" in many disputes, a formal complaint-handling process is set out. Unlike under the previous legislative framework, the NSA is not under an obligation to reach a statutory decision on every complaint it receives. Moreover, even if a complaint has been resolved informally to the satisfaction of

a complainant, the NSA may use its audit and investigatory powers if the complaint brought wider or systemic compliance issues to the attention of the NSA.

One of the more elaborate complaint-handling mechanisms is in place in the Netherlands where the NSA has published policy guidelines on how it will prioritise the handling of complaints. According to these guidelines, as a first step the NSA determines whether the complaint concerns the processing of personal data relating to the complainant, and whether basic desk research indicates that there is a clear violation of the GDPR. As a second step, if the desk research indicates that there may be a violation of the GDPR, the NSA assesses whether further investigation is necessary. In making this assessment, it takes account of several criteria cited in the Dutch report, including how harmful the alleged violation is for individuals; what the broader social significance of the case is; and the extent to which the NSA will be able to act effectively.

Thus, what emerges from the reports is a picture that is generally in favour of the strategic enforcement of the data protection framework. Concerns could be raised regarding the compatibility of such an approach with the right to an effective judicial remedy, since the strategic approach overrides the rights of individuals in some circumstances to ensure more effective protection for a greater number of individuals.[45] This concern was dismissed in the Netherlands in 2016 where the Administrative Jurisdiction Division of the Council of State, ruled that the pre-GDPR guidelines on complaint handling did not violate the Data Protection Directive nor the obligation to guarantee the effectiveness of EU law.

11 *How have these sanctions been applied by your NSA, and what additional sanctions have been adopted at national level in addition to those explicitly provided for by the GDPR?*

Introduction

The GDPR, unlike its predecessor, sets out detailed provisions relating to remedies, liabilities and penalties applicable pursuant to the regime. Of these penalties, the administrative sanctions set out in article 83 have received the most attention. This is because of the significant administrative fines they provide for: a maximum of €20 million or 4% of the annual global turnover of an undertaking, whichever is greater. The reports indicate that Member States have taken measures to limit the ability of NSAs to impose such administrative sanctions.

45 See, for instance, Centre for Information Policy Leadership, 'Regulating for results: strategic priorities for leadership and engagement', Discussion Paper, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement.pdf.

Limitation on the ability of the NSA to impose administrative sanctions

In both Denmark and Switzerland the NSA is unable to impose administrative fines. These administrative sanctions are criminal in nature for the purposes of human rights law and therefore attract all of the procedural safeguards attached to criminal procedures. In Switzerland, such criminal procedural guarantees are not regulated in the applicable Swiss administrative procedure, while in Denmark, only the courts can impose administrative fines. The NSA may also refer cases to the police for criminal prosecution, with two such referrals having been made under the GDPR.

Limitations on the discretion of the NSA when imposing fines are evident in other jurisdictions, in particular the amount of the fine is regulated in some Member States. In Portugal, the domestic law lowers the maximum amount of the administrative sanction foreseen by article 83 (4) and (5), taking into account the nature of the controller or processor (in particular, if the entity is an individual or an SME). It also provides that negligent infringements can only be sanctioned after the NSA has "advised" the controller to remedy the situation. Moreover, breaches of the data protection principles can only be sanctioned if they are intentional rather than negligent. The Portuguese report considers these limitations to constitute a breach of the GDPR. The Bulgarian legislature also differentiates between these upper limits and infringements that will lead to a sanction of no more than 2,500 euro.

Although not limited by law, the Czech NSA has made a concerted effort to inform the public through media and other public channels that the highest sanctions in the GDPR (article 83(4) and (5)) are envisaged for large multinational companies. It has indicated that it will continue to impose much lower fines in line with the upper limit under the previous data protection regime (386,000 euro). In Slovenia, domestic law does not place a quantitative limit on fines but provides, in line with article 83(1), that the fine imposed should not be a disproportionate or unprecedented burden on controllers or processors. The benchmark chosen for these purposes by Slovenian law, absent from the GDPR, is the sanction imposed for "comparable violations of human rights and fundamental freedoms".

Moreover, the requirement of a "warning in place of punishment" is common across Member States. The German report notes the very burdensome administrative procedures required to impose administrative fines and suggests that the reprimand provided for by article 58(2)(b) may act as a substitute in some circumstances. In Hungary, the law explicitly requires the NSA to issue such a warning before imposing an administrative fine to ensure the NSA exercises these powers in accordance with the principle of proportionality. A similar obligation is present in the Czech Act where it is "standard practice" for the NSA to impose a corrective measure before a fine and to impose such a fine only if the violation cannot be corrected, is grave or repeated.

While the Austrian act also requires such a "warning first" approach, the Austrian report suggests this requirement is not being followed by the NSA, which has imposed fines in several cases for first violations of the law.

A further potential limit on the ability of the NSA to impose administrative fines stems from article 83(7), which allows each State to "lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies". The possibility of imposing an administrative fine on a public body is precluded entirely in several Member States, including Croatia, Finland and Belgium. In Belgium, the Federation of Enterprises currently has a case pending before the Constitutional Court challenging this exclusion. The amount of the administrative fine is capped for public actors in other Member States, including Greece, Hungary, Malta and Sweden. In Romania fines can be applied to public actors provided priority is given to the "prevention mechanism", before resorting to them.

Additional sanctions at national level

The GDPR enables Member States to introduce "other penalties" for infringement of its provisions, subject to the proviso that they are effective, proportionate and dissuasive.[46] Many States have introduced – or retained – criminal sanctions.[47] This is the case in Belgium, France, Italy, Greece, Malta, Portugal, Switzerland and the UK, for instance. In Germany, both Federal and *Länder* data protection laws provide for criminal sanctions. The Austrian and Finnish laws specifically state that such sanctions can only apply where the illegal processing of personal data is not captured by article 83 GDPR.

Beyond criminal sanctions, additional regulatory powers and sanctions have been introduced. For instance, in Slovakia the NSA is empowered to impose a fine of up to 2,000 euro on persons who are not the controller or processor for failure to cooperate with the NSA. In the UK, the NSA now has the power to issue "assessment notices" which enable the ICO to access a company's premises and assess data protection practices much quicker than was previously the case. As the UK report notes, a 17-day delay occurred when the NSA requested a search warrant for its investigation into the use of personal data in political campaigns and to inspect the premises of Cambridge Analytica.

12 *Has your legal system historically awarded damages for intangible harm (in this area or others)? If so, how are such damages calculated?*

46 Art. 84(1) GDPR.

47 See, for instance, P. De Hert & G. Boulet, 'The Co-existence of Administrative and Criminal Law Approaches to Data Protection Wrongs' in D. Wright & P. De Hert (Eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches,* Cham, Springer, 2016, pp. 357-394.

The GDPR provides individuals with the right to receive compensation from a controller or processor for "material or non-material damage" suffered as a result of an infringement of the Regulation. The reports reflect on whether such a requirement is congruous with the domestic legal system and whether Member States had developed a practice for claiming such damages under the previous regime, which similarly provided for damages for intangible harm.

The acceptance of non-material harm within domestic legal orders

Historically, such damages have not been awarded in Slovakia, the UK and Ireland. In the UK and Ireland this issue has arisen in litigation before domestic courts, culminating in conflicting findings. In Ireland, the Irish High Court expressly held that, pursuant to domestic data protection legislation, a plaintiff would need to establish material loss in order to recover damages.

This can be contrasted with the findings of the English Court of Appeal in *Vidal Hall*. The Court considered the compatibility of a provision in domestic data protection law expressly limiting the right to claim damages for non-tangible harm under article 23 DPD. The latter provided more generally that any person who suffered damage as a result of unlawful processing was entitled to compensation for the damage suffered from the controller. The Court gave article 23 DPD its natural and wide meaning to include both material and non-material damage. As the national provision was not in conformity with this approach, the Court resorted to harmonious interpretation. Consistent with previous domestic case law, it held that:

> "In so far as a provision of national law conflicts with the requirement for an effective remedy in article 47, the domestic courts can and must disapply the conflicting provision".

This historic resistance to damages for non-material harm can be contrasted with other jurisdictions where compensation for such harm is well established. These jurisdictions are numerous and include Croatia, Denmark, Finland, Germany, Greece, Hungary, Malta, Norway, Luxembourg and Portugal. Such compensation goes by different names (for instance, "compensation for pain suffered" in Germany or "grievance awards" in Hungary). The particular fields of law where such compensation may be awarded may be specified, for instance in Malta the most notable cases deal with human rights, defamation and intellectual property law.

One theme that emerges from these reports is that the compensation awarded is often very low, often symbolic, monetary sums (as noted by Finland and Norway). In Belgium,

compensation for moral damage can also be granted in kind. The publication of the judgment in which the harm was recognised may constitute compensation and the national report notes that, "legal costs will often outweigh the benefit that can be gained from a claim for compensation, resulting in little caselaw on the matter".

Damages for data protection violations

Given that the former data protection framework also provided, albeit implicitly, for such damages, it is interesting to consider how these actions for such damages have developed at national level.

There have been a number of cases in Sweden. For instance, in a case where a person used their website to accuse five people of rape, damages of approximately 500 euro each were awarded to the data subjects. In Belgium, a court awarded 750 euro to an employee whose employer had installed a track-and-trace system in his company car allowing the employer to follow his every movement (including outside working hours) without informing him adequately.

Proving that such harm has occurred can be challenging for data subjects. The Italian report contends that a mere violation of the data protection code does not suffice for a compensation claim: the seriousness of the injury and the damage suffered must be assessed. This issue is not addressed by the GDPR and there is no consistent practice across Member States, falling as this does to national law. The Spanish report notes that under previous law, damage was presumed and awarded whenever there was a breach, however, the current law indicates that the data subject must prove the damage. In Luxembourg however the court's jurisprudence suggests that harm in the context of infringements of personality rights is not rigorously controlled once fault is established. Whether or not Member States adopt this approach more generally in the data protection context remains to be seen.

Finally, establishing a quantum of damages is challenging in this context. In Austria it is possible that this will be "determined by free judicial conviction" and in such cases, the circumstances of the case will be equally important as the harm to the victim. In Greece, the former law set a minimum amount of compensation for intangible harm at 5,869.40 euro. However, this minimum amount was deemed to be unconstitutional by the Greek courts that considered it to be incompatible with the principle of proportionality.

Given the reluctance of States to award significant damages for intangible harm under the DPD, it would seem that the award of greater damages for such harm under the GDPR is unlikely. Moreover, with limited prospects for such damages, individuals may decide that the game is simply not worth the candle and refrain from legal proceedings. One potential alternative, now considered, is for representative actions to litigate on behalf of individuals.

13 *Has your Member State introduced legislative measures to facilitate such representative actions? What role have NGOs played in data protection enforcement in your State and are there any alternative movements emerging at national level (such as personal data cooperatives or unions) to combat such asymmetries?*

Article 80 GDPR provides for the "representation of data subjects". Article 80(1) GDPR awards data subjects a right to mandate a properly constituted non-profit entity to lodge a complaint on their behalf with an NSA or to seek an effective judicial remedy against a data controller, processor or an NSA. This is the compulsory part of article 80.

However, article 80 also leaves two choices to Member States. First, article 80(1) states that where provided for by national law the data subject may mandate the non-profit entity to seek compensation on their behalf. Second, also where provided for by law, article 80(2) allows for such representation without the mandate of the data subject. Before considering how these provisions have been received in Member States, it is useful to consider the background context.

Representative mechanisms existed pre-GDPR

Mechanisms involving representation by others were already in place under domestic law in some countries, such as Croatia and Denmark, prior to the entry into force of the GDPR, and therefore no new legislative actions have been taken pursuant to article 80.

However, in other States while some mechanisms for representative actions exist, they do not necessarily apply in the data protection context. For instance, in both Malta and Poland, such actions are possible in situations specifically enumerated in domestic law. While the authors of both reports indicate that there is support to extend the scope of application of such actions to avail of the possibility afforded by the GDPR, domestic law has not yet been extended to do so. Similarly, in Spain and particularly in Germany the possibility exists to pursue data protection claims under the auspices of the civil enforcement of consumer protection law. However, the German report notes that this collective action right of consumer organisations (*Verbraucherzentralen*) is not to be understood as an implementation of article 80. This failure to extend existing mechanism to incorporate data protection actions, or to introduce new mechanisms, seems to fall foul of the article 80(1) requirement to introduce this possibility for data subjects.

Availing of the flexibilities in article 80 GDPR

It appears that the majority of Member States have not opted to enable non-profit actors to seek compensation on behalf of the data subject following a mandate. This possibility

has been availed of in France. The Austrian report notes that while it was originally intended to extend domestic law to cover such actions, this was ultimately not included in the Act. This exclusion has been viewed critically by activist organisations such as Austrian noyb (none of your business).

Similarly, it seems that the possibility of enabling representation without a mandate has not been widely availed of. Again, a notable exception here is France, which not only incorporates the possibility envisaged by article 80(2) into national law but also extends this to matters of compensation. Therefore a non-profit organisation may seek compensation on behalf of a data subject even without their mandate pursuant to French law.

Properly constituted organisations

The GDPR specifies that the not-for-profit body, organisation or association (hereinafter "NGO") be "properly constituted in accordance with the law of the Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data".

It is clear that Member States have sought to add further conditions to these three criteria, in a manner that is probably incompatible with EU law. For instance, under Czech law the person acting on behalf of an NGO in civil or administrative proceedings must have a "full legal education". It seems that there is no such requirement if the data subject decides to be represented by a natural person.

In France, relevant associations must have been established for at least five years. As the French report notes, no such temporal limitation exists in the GDPR and this requirement stems from a previous French law.

As the Romanian report indicates, the form in which the NGO receives the mandate may also influence the feasibility and legality of such representative actions. It would seem that in Romania such mandates must be issued under law by a lawyer or a notary.

Representative activity at domestic level

Representative actions in the field of data protection still remain relatively uncommon at national level. There has however been notable litigation in the consumer protection context. In Belgium, seven of the eight collective actions instigated since the relevant law entered into force in 2014 were initiated by Test-Achats, a consumer protection organisation. One of these actions was pending before the Brussels commercial court in

the wake of Facebook's data breach of September 2018 and the Cambridge Analytica scandal, according to the national report.

In the UK there has also been more activity in recent years. For instance, in *WM Morrisons Supermarkets plc v Various Claimants* the Court of Appeal considered the vicarious liability of a supermarket for the deliberate disclosure by one of its employees of the payroll data of 100,000 employees on a file sharing website. The judgment confirming the vicarious liability is currently under appeal before the Supreme Court. Some claimants in this case were part of a group legal order, which is recognised when a number of claims give rise to common or related issues of fact or law. The national report also indicates that a similar order may be prepared in respect of the British Airways data breach referred to earlier.

Where such initiatives are absent, this may be explained in part by the lack of domestic civil society actors active in this field. This absence has been noted in relation to several countries, including Bulgaria, Denmark, Greece and Slovenia. Indeed, the Slovenian report notes that at present there is no registered organisation that would meet the requirements of article 80.

More positively, where such civil society organisations are well established, they have made a significant impact. For instance, in the Netherlands civil society campaigned for the organisation of a consultative referendum on the Dutch Intelligence and Security Services Act. Some 6.7 million Dutch inhabitants voted in this referendum, with a majority voting against the Act. Although the referendum was not binding, the government did adjust the law to address some of the public concerns. In Belgium, two NGOs are currently appealing an Act before the Constitutional Court that embeds a fingerprint in new identity cards.

As the Czech report indicates, the role of civil society is not limited to assisting in and lodging formal complaints and judicial proceedings. It includes public information campaigns, submissions of comments on draft legislation and the granting of awards and "anti-awards". Moreover, the variety of actors engaging in data protection advocacy is expanding. In Austria, the Chamber of Labour acts as an advocate for higher data protection standards and has published various reports on related issues. In France, there is now a trade union to represent data protection officers who are multiplying in number across organisations.

14 *Have these trends been visible in your Member State? In particular, has the NSA cooperated with other regulators or an ombudsperson formally or informally?*

Personal data is the object of multiple legal and regulatory frameworks leading to potentially competing claims regarding how its processing should be regulated and by whom. Moreover, just as digital data does not respect territorial boundaries, it also challenges

traditional boundaries between regulatory authorities. States have therefore been considering whether existing institutional arrangements are up to the task of effective regulation in the digital context.

What emerges from the national reports is that cooperation between regulatory agencies is the norm rather than the exception. Such cooperation is reported as being entirely absent only in Slovakia and Austria. Indeed, NSAs actively seek such cooperation. For instance, in its Regulatory Action Plan approved by parliament in November 2018, the UK NSA set out the objective to "work with other regulators and interested parties constructively, recognising the [… interconnected] nature of data flows in the expanding digital economy".

Nevertheless, while such cooperation is occurring more frequently, there is little consistency with regard to which regulatory agencies cooperate and the basis for their cooperation.

Formal cooperation

Many reports note that while such cooperation exists, it is "informal and ad hoc" as in Malta or "entirely based on personal relationships" like in the Czech Republic. In recent years, one of the more visible avenues for more formal cooperation between regulatory authorities has been the "Digital Clearinghouse" launched by the European Data Protection Supervisor with a view to facilitating dialogue and cooperation on data protection and consumer protection, and between competition authorities and, more recently as noted in the Institutional Report, electoral regulators. The reports from Ireland and Luxembourg note the participation of the NSA in this forum.

Indeed, cooperation between these particular authorities is increasingly visible. The German report refers to the legislative amendment that brought data protection law within the scope of application of competition law, allowing the German Competition Authority to initiate proceedings against Facebook for an abuse of dominance through its failure to respect data protection law.

In Ireland the updated Consumer Protection Regulations entered into force in January 2020. They enable competent authorities to request the exercise of enforcement powers by other competent authorities. Moreover, the domestic data protection legislation specifically recognises the importance of collaboration between regulators and other statutory bodies at both domestic and international level. It creates an exemption to the general prohibition on the disclosure of confidential information by staff of the NSA if such disclosure is made "to a public authority, whether in the State or otherwise, for the purposes of facilitating cooperation between the Commission and such authority in the performance of their respective functions".

What is perhaps less expected is the reference to agencies with ostensibly similar missions to NSAs in the German and Greek reports. The German report notes that data protection is tightly linked to data security and, as such, the Federal Office for Information

Security plays a role in the wider context of data protection. Similarly, in Greece an Authority for Communication Security and Privacy exists alongside the NSA and their relationship is governed by law.

Filling the gaps?

While the idea of creating designated regulators for the internet is garnering public attention, there is little evidence of such institutional change in the reports. Malta has created a new authority – the Malta Digital Innovation Authority – to "regulate innovative technologies". However, other reports note the adequacy of the status quo: for instance, the German report notes that strong authorities already exist at federal and *Länder* level with corresponding far-reaching competences.

Rather, what we see is cooperation between authorities to fill gaps in their competences in some circumstances. In Poland, the NSA cooperates with the national ombudsman as the latter has additional useful competences, such as the ability to lodge complaints to the Constitutional Court. Similarly, in Finland, consumer authorities have the competence to commence group complaints and class actions of their own initiative, competences the NSA does not possess. In France, regulatory authorities have worked together on different themes such as knowledge management, human resources and using data to inform regulation. A report was published on the latter in July 2019.

15 *Is "national security" defined in your domestic law or administrative practice? Have national authorities accepted the application of the EU Charter to data retention for national security purposes (following from the* Tele2 and Watson *judgments)?*

Introduction

In *Digital Rights Ireland* the CJEU annulled the EU Data Retention Directive in its entirety on the basis of its incompatibility with the Charter rights to privacy and to data protection.[48] The CJEU considered that the Directive went further than was necessary to achieve its objective of combatting serious crime by not setting out clear and precise rules regarding the extent of the interference with these rights.

The compatibility of data retention requirements with fundamental rights had concurrently been the subject of legal challenges across several EU Member States, with national jurisdictions struggling to gauge the implications of *Digital Rights Ireland* for

48 Judgment of 8 April 2014 in Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

their domestic data retention legislation. It was against this background that *Tele2/Watson*[49] was delivered. This judgment marked a significant shift in approach as the CJEU held that the objective of fighting serious crime cannot "in itself justify the finding that general and indiscriminate data retention legislation is necessary for the fight against crime".[50] Thus, general and indiscriminate data retention was deemed to be incompatible with the Charter rights, irrespective of the safeguards put in place around access and use amongst other things. This judgment has proven to be divisive, as the reports reflect. Moreover, as the reports also reflect, the current legal landscape is a dynamic one, with references pending relating to its application in the criminal context from the Estonian Supreme Court[51] and, most recently, the Irish Supreme Court.[52]

The reception of Tele2/Watson into domestic legal orders

Austria has set the gold standard for the reception of *Tele2/Watson* into domestic legal. In 2018, Austria introduced amendments to relevant legislation in order to implement a "quick freeze model", which means that in the event of an initial suspicion of certain criminal offences, telecommunications providers should be required by public prosecution to retain telecommunications data stored. Furthermore, the Austrian law provides that access to these data is only permissible on the condition of a specific suspicion regarding an offence and judicial authorisation. The explanatory notes for these amendments refer to *Tele2/Watson* several times, reflecting the willingness of the legislature to adjust national law accordingly. In Sweden legislative changes have been introduced in response to the judgments, while such amendments are in the pipeline in Luxembourg.

In Germany, doubts were raised regarding the compatibility with EU law of domestic data retention provisions enacted to reflect *Digital Rights Ireland*. These rules were supposed to enter into force in July 2017. However, a regional court shared these concerns and discharged a single operator from its storage obligations. This in turn led the Federal Network Agency to suspend the implementation of these obligations.

These efforts can be contrasted with the situation in Italy where, despite a request from the NSA to the legislature to amend the legislative text, an Italian law contains an exception for data retention in order to ensure the effectiveness of investigative tools for counter-terrorism purposes and the repression of specified criminal offences.

---

49 Judgment of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, ECLI:EU:C:2016:970.

50 Ibid, para. 103.

51 Request for a preliminary ruling from the Riigikohus (Estonia) lodged on 29 November 2018, Case C-746/18, *H.K. v Prokuratuur*.

52 *Dwyer v The Commissioner of An Garda Siochana and Others* (2019/18, Irish Supreme Court).

The extension of Tele2/Watson to national security

The prohibition of general and indiscriminate data retention set out in *Tele2/Watson* was provided for in the context of data processing for the purposes of fighting serious crime. However, the question has arisen of whether this prohibition on indiscriminate data retention also applies in the context of national security.

One could argue that the dividing line between policing serious crime, protecting public order and security, and protecting national security is becoming increasingly blurred. The Charter also applies to Member States when availing of exceptions set out in EU legislative instruments, arguably including national security. Nevertheless, article 4(2) TFEU ostensibly excludes national security from the scope of application of EU law, although – as the Institutional Report clearly indicates – the meaning of article 4(2) remains contested. It is therefore little wonder that a number of preliminary references are now pending before the CJEU querying the outer limits of the *Tele2/Watson* judgment.

The questions referred from France and the UK, and the accompanying text, reflect what the French report considers to be a great reluctance to apply the *Tele2/Watson* conditions. In particular, the French *Conseil d'Etat* considers that data retention is necessary to tackle threats. It asked the Court to consider whether the data retention obligations must be considered in the context of the serious and persistent threats to national security, and in particular terrorist threats, and therefore be viewed as a justifiable interference to ensure the right to liberty and security provided for in the Charter, and the demands of national security that Member States are responsible for.[53] Similar questions were concurrently posed by the UK Investigatory Powers Tribunal in the *Privacy International* referral[54] and subsequently from the Belgian Constitutional Court.[55]

The Dutch Courts have refused to consider the possibility that the *Tele2/Watson* reasoning applies to national security on several occasions, indicating that when personal data are processed by a private party, but are destined for use by one of the intelligence services, this does not fall within the scope of EU law. Similarly, the Czech national authorities have actively argued against the view that *Tele2/Watson* could be extended to data retention for national security purposes. However, even if EU law does apply to such processing, it claims that conditions for proportionality would need to be vastly different from *Tele 2/Watson*, due to the different nature of threats against national security and

53 Request for a preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018, Case C-511/18, *La Quadrature du Net and Others.*

54 Request for a preliminary ruling from the Investigatory Powers Tribunal, London (United Kingdom) lodged on 31 October 2017, Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others.*

55 Request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 2 August 2018, Case C-520/18, *Ordre des barreaux francophones and germanophone and Others.*

the different nature of the instruments needed to prevent these threats. The government's position has found support from the Czech Constitutional Court, which has recently ruled that the general data retention obligation is in accordance with the Czech constitution, even for the purposes of prevention, investigation, detection and prosecution of criminal offences.

Future perspectives

It is neither possible nor desirable to attempt to draw firm conclusions based on this General Report. Yet, a number of important themes can be gleaned from the excellent reports, both national and Institutional, that merit further discussion.

First, in this area as in many others of EU law, the tension between regulatory convergence and harmonisation, on the one hand, and respect for the constitutional and legal plurality of EU Member States is ever present. The GDPR is an unusual legal instrument, as an EU *regulation* it leaves considerable margin for manoeuvre to Member States in a way that detracts from its harmonising ambitions. The need for its "reception" in domestic legal orders is more akin to the implementation of a directive than the direct applicability of a regulation and makes for a complicated legal landscape at domestic level.

The use of this discretion in areas touching upon national constitutional rights, such as freedom of expression, and sovereign prerogatives, such as national security, may be viewed as essential to avoid clashes between domestic constitutional courts and the CJEU, where possible. This may explain the CJEU's cautious approach when providing guidance on how data protection should be reconciled with freedom of expression, leaving this balancing to a large extent to national courts and authorities. Whether such a restrained approach is taken in the national security context remains to be seen.

A second theme that emerges relates to the enforcement of the European data protection framework. While EU legislation has always provided for robust substantive data protection, these provisions have not been enforced, leading to a visible gap, perhaps more accurately a chasm, between the law "on the books" and in practice. Enhancing enforcement was one of the key EU data protection reform priorities and led to the introduction of mechanisms such as the one stop shop and the creation of a new EU body, the EDPB. Since the GDPR's entry into force, domestic authorities have seen a significant increase in demand for their regulatory assistance at domestic level, on top of their increased "European" duties. While many have strategic plans in place to prioritise their workloads, it remains critical that these authorities remain adequately resourced. It is still too early to assess whether the new regime will lead to improved enforcement.

Many of the complementary mechanisms introduced to support this public enforcement, including the possibility for representative actions on the part of the data subject and the

continued availability of damages for intangible harm, do not appear to be having a significant impact across Member States as of yet. Indeed, it is in neighbouring areas, such as consumer protection, that representative actions are having the most bite.

A third theme to highlight is the ongoing tussle between dual visions of personal data, namely as a commodity, and as an extension of the personality and dignity rights of individuals. It is clear that at EU level there is little desire to renege on the commercial benefits of personal data processing. Yet a commitment to data protection is required under the Charter. This explains the prevarication regarding how personal data should be treated in the Digital Content Directive, for instance. This is also evident at national level where there is no uniform approach to key questions such as whether consent can be "free" when the provision of a service or content is made conditional on such consent. This validates Cohen's approach to the information economy: it is not possible to disaggregate data processing practices from the business models they sustain.[56] This is an issue that may test the EU's commitment to the right to data protection in the future.

56 J. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP, 2019).

Institutional Report Topic 2: The New EU Data Protection Regime

Anna Buchta and Herke Kranenborg[*]

1 Introduction

It will not have gone unnoticed that new data protection rules became applicable in the EU in May 2018. As data subjects, people were flooded with information and consent notices. As persons in charge of data processing activities, there was great compliance stress, at all levels from schools and sports clubs to public administration to small, medium and big enterprises. One thing can safely be concluded: the General Data Protection Regulation (hereinafter "GDPR") has been a huge success in creating awareness of the existence of data protection rules. Data protection rules to a large extent were not really new. The 'game changer' was the introduction of the power for data protection authorities to issues fines up to 4% of the annual worldwide turnover.

The FIDE 2020 conference, after two years of GDPR, is an excellent opportunity to take stock and look at where the Union stands with regard to its data protection regime. It should be noted that the data protection regime covers more than the GDPR only. In May 2018, EU Member States also had to transpose Directive (EU) 2018/680 which contains data protection rules for law enforcement authorities (hereinafter "Law Enforcement Directive"). Moreover, there are specific data protection rules for the telecoms sector and for EU institutions and bodies. In addition, several EU instruments in the area of freedom, security and justice have specific data protection provisions.

In order to keep the exercise within reasonable limits, the questionnaire for the present topic highlighted more specific themes, and focuses on several topical legal issues. The present report follows the main structure of the questionnaire and looks at the different issues from a purely EU perspective through focus on relevant activities of the EU legislator; on the supervision of EU data protection rules at EU level; and on topics which were the subject of recent rulings of the Court of Justice of the European Union (hereinafter "CJEU").

---

* Respectively Head of Unit Policy and Consultation, European Data Protection Supervisor; Member of the Legal Service, European Commission, Professor of European Data Protection and Privacy Law, Maastricht University, and affiliated member of the Institute of European Law, KU Leuven. The opinions expressed in the report reflect the authors' personal opinions and cannot be attributed to the EDPS or the European Commission.

2 Setting the scene

Since the entry into force of the Lisbon Treaty in December 2009, the right to protection of personal data is firmly grounded in primary Union law. The right is laid down in article 16 of the Treaty on the Functioning of Europe (hereinafter "TFEU") as well as in article 8 of the Charter of Fundamental Rights of the European Union (hereinafter "Charter"), next to the right to privacy in article 7. Article 16 TFEU also provides a self-standing legal basis for data protection rules in all areas of Union law.[1] The provision lies at the basis of the GDPR and the Law Enforcement Directive, as well as Regulation 2018/1725 for the Union institutions and bodies. The development of the Union *acquis* on data protection is continuing, *inter alia,* with the pending legislative procedure on a new ePrivacy Regulation.

Recent years have also shown the CJEU as a driving force behind upholding strong, harmonised data protection standards in the Union. Following an analysis in the light of articles 7 and 8 of the Charter, the Court has declared several Union instruments invalid and has given a negative opinion on a draft agreement between Canada and the Union on transfer of Passenger Name Records. Also national supervisory authorities and the European Data Protection Supervisor, including through their participation in the former article 29 Working Party (now the European Data Protection Board), have contributed to the understanding and consistent application of the EU data protection rules.

The European Commission has taken stock of the implementation of the GDPR in two communications in which it concluded that while the overall picture is positive, further progress remains necessary in a number of areas, amongst which are the allocation of sufficient resources to national supervisory authorities and the cooperation between them.[2] At the time of writing the Commission was preparing a report on the evaluation and review of the GDPR.[3]

The European Commission also used the occasion of the new data protection rules to expand more actively the international dimension of Union data protection, relying on the growing trend at global level to raise the protection of individual data in the digital era.[4] In 2019, for example, the Commission adopted a new adequacy decision concerning Japan, and negotiations or exploratory talks are taking place with South Korea and several Latin American countries.[5] The Commission also developed specific provisions on data

1 Art. 39 TEU contains a specific procedure for the adoption of data protection rules for the common foreign and security policy.

2 Communication COM(2018)43 of 24 January 2018, Stronger protection, new opportunities, and Communication COM(2019)374 of 24 July 2019, Data protection rules as a trust-enabler in the EU and beyond – taking stock, p. 18.

3 As required by art. 97 GDPR.

4 Communication COM(2017)7 of 10 January 2017, Exchanging and protecting personal data in a globalised world.

5 Communication COM(2019)374, part VI.

flows and data protection for trade agreements, which it systematically tables in its bilateral and multilateral negotiations. These horizontal rules are intended to rule out purely protectionist measures, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection.[6]

3 GDPR responsibilities: Consent and controllership

3.1 Consent

Pursuant to article 8(2) of the Charter, personal data may only be processed 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. Article 6 GDPR exhaustively lists the grounds for lawful processing, the first being where the data subject has given consent for one or more specific purposes.[7] Consent must be freely given, specific, informed and unambiguous.[8]

Although no ground in article 6(1) has normative priority over the others, in practice consent may play a salient role in the private sector whenever no other legal basis seems appropriate.[9]

The conditions for "specific", "unambiguous" and "informed" consent were clarified by the CJEU in *Planet49*.[10] The case concerned the consent of participants in a promotional online lottery to the sharing of their data with the company's sponsors and partners, as well as to the storage and reading of cookies.

The Court confirmed that only active behaviour on the part of the data subject with a view to giving their consent (and not, for example, a pre-ticked box) fulfils the requirement of "unambiguous" consent.[11] Consent must also relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes.[12] The ruling suggests that informing users that through continuing their activity on a website ("continuous browsing") they consent to the placing of cookies on their devices is not sufficient for the consent to be valid.

In *Planet49*, the question also arose whether consent to the processing of personal data for advertising purposes could be considered as "freely given" when it was a prerequisite

6 Ibid, p. 12.
7 Art. 6(1)(a) GDPR.
8 Art. 4(11) GDPR.
9 See W. Kotschy, commentary on Article 6 GDPR in C. Kuner et al. (Eds),*The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2019.
10 Judgment of 1 October 2019 in Case C-673/17 *Planet49 GmbH*, ECLI:EU:C:2019:801.
11 Ibid, para. 54.
12 Ibid, para. 58.

for the user's participation in a lottery. An answer to this question would have affected the majority of online publishers and service providers that condition access to their services on allowing online behaviour tracking through cookies or reliance on "cookie walls" as a source of income. AG Szpunar did not rule it out and even referred in his Opinion to "selling" of personal data in the sense of "agreeing to be contacted by so-called sponsors [of an on-line lottery] for promotional offers".[13] However, the Court chose not to engage with this issue in its ruling[14] and so the validity of "cookie walls" and similar business models remains unresolved as a matter of EU law.

The monetisation of personal data is a recurring subject of debate. It is widely accepted today that personal data may have monetary value and in many cases they are traded as a commodity, often as part of large data sets.[15] An analysis of this economic dimension of the data economy was provided by the European Data Protection Supervisor (hereinafter "EDPS") back in 2014.[16] Since then, monetary value of personal data has been recognised explicitly in certain Union instruments.[17] Also the proposal for the ePrivacy Regulation acknowledged that "[i]n the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements".[18]

In the context of the legislative process leading to Directive (EU) 2019/770 on digital content, the EDPS sharply criticised the introduction of the notion of "personal data as counter-performance" in the proposal,[19] considering that since personal data are related to a fundamental right, they "cannot be considered as a commodity" or "conceived as a mere economic asset".[20] The EDPS also demonstrated how the very literal conception of "data as currency" was bound to raise difficult questions about the relationship of the proposed Directive and the relevant provisions of the GDPR (in particular with respect to lawful bases for processing). The final text of Directive (EU) 2019/770 sends mixed messages. It recognises that "the protection of personal data is a fundamental right and

13 Opinion of AG Szpunar of 21 March 2019 in Case C-673/17 *Planet49 GmbH*, ECLI:EU:C:2019:246, para. 99.

14 C-673/17 *Planet49*, para. 64.

15 Report of J. Crémer, Y-A de Montjoye and H. Schweitzer of 2019 for the European Commission, *Competition policy for the digital era*, www.ec.europa.eu/competition/publications/reports/kd0419345enn.pdf, p. 2. This webpage and those following were visited on 1 February 2020.

16 EDPS preliminary Opinion of March 2014, www.edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

17 See for example recital 16 of Directive (EU) 2018/1972 establishing the European Electronic Communications Code (recast) [2018] OJ L321/36.

18 COM(2017)10 final, rec. 18.

19 EDPS Opinion 4/2017 of 15 March 2017, https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en_1.pdf.

20 Ibid, p. 7.

that therefore personal data cannot be considered as a commodity",[21] but, at the same time, the scope of the Directive does include situations where "the consumer provides or undertakes to provide personal data to the trader".[22]

It seems indeed that the notion of "personal data as counter-performance" oversimplifies complex realities and fails to account for the various business models that exist. Equating "paying a price" with money is often misleading, if only because the average consumer would typically not be in a position to fully understand how exactly the information related to him is processed and how much value is actually extracted from it.[23] Moreover, adopting such concepts in legislation (or case law) may inadvertently serve to legitimise business practices which are questionable, if not illegal, under the GDPR.

Also the European Data Protection Board (hereinafter "EDPB") appears to confirm that it is necessary to make a distinction between certain business practices and their compatibility with data protection rules.[24] As technological progress has increased the possibilities to process growing amounts of personal data, online service providers have been incentivised to maximise their data collection and use, including through contractual terms – which, according to the EDPB, constitutes an "acute risk".[25] Furthermore, article 6(1)(b) GDPR (processing necessary for a contract with the data subject) cannot provide a lawful basis for online behavioural advertising simply because such advertising funds the provision of the service. Additional elements would need to be considered to establish the necessity of such processing. Relevant factors may include the mutual perspectives and expectations of the parties, including whether an ordinary user of the service would reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract.

It is difficult to dispute the fact that data – including personal data –are necessary for the development and functioning of many services and products that are indispensable in a modern society. Attempts to assign monetary value to data are therefore understandable from the point of view of economics. A broader reflection is still needed about the compatibility of "data monetisation" approaches with the fundamental right nature of personal data protection.

21 Recital 14 Directive (EU) 2019/770 [2019] OJ L136/1.

22 Ibid, art. 3(1), second paragraph.

23 This is partly due to the fact that standard contractual terms and privacy policies typically contain vague terms like "improving consumers' experience" and are practically never explicit about the actual ways of monetising information.

24 See EDPB Guidelines 2/2019 of 9 April 2019, www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

25 Ibid, p. 6.

3.2 Controllership

The concept of "controller" is key to determining who is responsible for compliance with the data protection rules, including against whom data subjects can exercise their rights and, in many cases, which supervisory authority is competent. Controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[26]

Today, the roles of controllers and processors (who process data on behalf of the controller) are becoming more fluid, with controllers losing some of their traditional dominance over data and processors being more likely to influence decisions over it (as, for example, in the field of cloud computing). This might explain why the concept of "joint controllers" is gaining importance.

Article 26 GDPR clarifies that two or more controllers who jointly determine the purposes and means of processing, are to be considered joint controllers. Further, it imposes on such joint controllers an obligation to enter into an arrangement setting out their respective responsibilities, in particular in relation to the modalities for the exercise of data subject rights and transparency obligations. The designation of a contact point for data subjects may be covered by such an arrangement. Still, data subjects are able to exercise their rights in respect of each of the joint controllers.[27]

Joint controllership was also considered by the CJEU. In *Wirtschaftsakademie* a private-law company operating in the field of education was ordered to deactivate its fan page on Facebook, since the personal data of the visitors of the fan page were collected via cookies without informing them.[28] Wirtschaftsakademie argued that it was not the controller in relation to this processing, but that Facebook was.

The Court applied a broad interpretation of the concept of "controller". By setting up the fan pages on Facebook's terms, setting the parameters and allowing Facebook and others to place cookies, the administrator of such pages contributed to the visitors' personal data processing and therefore became controller, jointly with Facebook Ireland.[29] The fact that the fan page administrator did not have access to the personal data but only received anonymised statistics did not prevent joint controllership.[30] The Court underlined that "the existence of joint responsibility does not necessarily imply equal responsibility of the

26 Art. 4(7) GDPR.

27 Art. 26(3) GDPR. The EDPS issued guidelines on the concepts of controller, processor and joint controllership as regards Union institutions and bodies. See EDPS Guidelines of 7 November 2019, www.edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

28 Judgment of 5 June 2018 in Case C–210/16, *Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388.

29 Ibid, para. 36.

30 Ibid, para. 38.

various operators involved in the processing of personal data" but that the "level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case".[31]

The Court's ruling may have far reaching consequences for users of any service or platform which technically permits the collection and processing of personal data, e.g. by placing cookies or similar tracking devices, or by allowing the collection of IP addresses. In such cases, by agreeing with terms and conditions for use of the tool, the users may be taking part in the determination of the purposes and the means of data processing, thus becoming joint controllers for such data processing activities. Regarding in particular the arrangements between joint controllers required under article 26 GDPR, it remains to be seen to what extent an individual administrator of a Facebook fan page (or any user of another tool or platform offered by a large company) has any leverage in shaping the respective obligations in such an un-balanced relationship.

The Court confirmed its broad understanding of "controllership"' in *Jehovan todistajat* in relation to the collection of personal data by the Jehovah's Witnesses in the course of their door-to-door activities.[32] The Court clarified that in order to qualify as a controller there is no need for providing guidelines or instructions.[33] Nor must the data controller necessarily have access to the data processed. It must be determined in practice whether the actor exerts sufficient influence over the processing of data so as to qualify as a data controller.[34]

In *Fashion ID*, the CJEU further clarified the concept of (joint) controllership.[35] The case concerned the responsibility of the operator of a website embedding on its website the "Like" social plug-in (button) from Facebook. Through the "Like" button, personal data of people accessing the website, such as IP addresses and website history, were sent to Facebook, regardless of whether the user clicked on it or was himself a member of Facebook. The Court found that Fashion ID was joint controller with Facebook with respect to two stages of the processing: the collection of personal data and disclosure by transmission of those data.[36] The website operator was found to exert decisive influence over the processing, since the collection and transfer would not occur if the plug-in had not been embedded.[37] At the same time, the website operator's responsibility as controller is limited to the operation or set of operations for which it actually determines the purposes

31 Ibid, para. 43.
32 Judgment of 10 July 2018 in Case C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551.
33 Ibid, para. 67.
34 Ibid, para. 68. See on the ruling R. Gellert, 'Door-to-Door Preaching by Jehovah's Witnesses Community falls under Data Protection Law', *EDPL*, Vol. 4, No. 3, 2018, pp. 391-395.
35 Judgment of 29 July 2019 in Case C–40/17, *Fashion ID GmbH*, ECLI:EU:C:2019:629.
36 Ibid, para. 84. On this point, the Court followed the Opinion of AG Bobek of 19 December 2018, ECLI:EU:C:2018:1039.
37 Ibid, para. 78.

and means, that is to say, the collection and disclosure by transmission of the personal data at issue.[38]

Fashion ID is the first case in which the Court assigned specific responsibilities in a situation of joint controllership based on the data processing stages in which a controller is involved. This "phase-oriented" approach to the division of responsibilities between joint controllers has been criticised for lacking clear underpinnings in Union data protection law (e.g. the list of examples of processing operations in article 4(2) of the GDPR, to which the Court referred, was never intended as a systemic classification of the different phases of data processing) and for possibly exacerbating legal uncertainty. In addition, limiting responsibilities to individual phases of data processing might result in losing sight of the bigger picture, when it comes to the societal risks posed by complex, networked, personal data processing systems such as in the case of a service provider like Facebook.[39]

4 GDPR rights: Data protection, freedom of expression and the right to be forgotten[40]

4.1 Data protection and freedom of expression

The right to data protection has a dual relationship with the freedom of expression which, according to article 11 of the Charter, includes the freedom to receive and impart information. On the one hand, data protection rules aim to reach a harmonised level of data protection ensuring the free flow of information. On the other hand, data protection rules might require a restriction of the public disclosure of personal data. The development of the information society made the friction between the two rights increasingly apparent.

The potential conflict between both rights is recognised in article 85 GDPR which requires Member States to provide, by law, for exemptions or derogations from the GDPR for processing carried out for "journalistic purposes" or the purpose of academic, artistic or literary expression, if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information. Exemptions or derogations are possible from almost all provisions of the GDPR, but not with regard to judicial

38 Ibid, para. 85.

39 R. Mahieu and J. van Hoboken, 'Fashion-ID: Introducing a phase-oriented approach to data protection?', European Law Blog, https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/.

40 See also the commentary of H. Kranenborg on articles 17 and 85 of the GDPR in C. Kuner et al. (Eds), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2019 and the commentary of H. Kranenborg on article 8 of the Charter in the upcoming second edition of S. Peers et al. (Eds), *Commentary on the EU Charter of Fundamental Rights*, Oxoford, Hart Publishing.

remedies, liability and sanctions.[41] A similar provision existed in the former Directive 95/46/EC.[42]

Whether the EU data protection rules as such brought about an unjustified restriction of the freedom of expression was addressed in the *Lindqvist* ruling of 2003.[43] It concerned the publication on a Swedish internet site of certain personal information by Mrs Lindqvist about fellow parishioners in her church. The Court did not consider that the former Directive 95/46/EC in itself restricted the freedom of expression and that it was for the national authorities and courts responsible to apply the transposing national law in such a way as to ensure a fair balance between the rights and interests in question, including respect for fundamental rights.[44]

In later rulings, the CJEU gave a very broad interpretation to the notion of 'journalistic activities', thereby allowing Member States a large margin of manoeuvre. In *Satamedia*, the Court considered that activities could be classified as journalistic if their object was the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them.[45] In *Buivids*, the Court considered that not all information published on the internet, involving personal data, comes under the concept of "journalistic activities".[46] Uploading a film on YouTube can be done solely for journalistic purposes, provided its sole objective is the disclosure to the public of information, opinions or ideas.[47]

According to article 85 GDPR, exemptions or derogations from the GDPR should be made if "necessary to reconcile" the right to the protection of personal data with the freedom of expression and information which requires a balancing of the two rights. The CJEU has been cautious in giving substantive guidance. In *Buivids*, the CJEU made reference to the case law of the European Court of Human Rights (hereinafter "ECtHR") on reconciling the rights to privacy and freedom of expression and the relevant criteria developed by that Court for the balancing exercise.[48]

In its case law, the ECtHR paid particular attention to the public status of the persons involved. Persons who have entered the public arena, such as politicians, are required to

41 See Chapter VIII of the GDPR. Chapters I, X and XI are also excluded.

42 Article 9 Directive 95/46/EC.

43 Judgment of 6 November 2003 in Case C-101/01, *Lindqvist*, ECLI:EU:C:2003:596, para.72.

44 Ibid, para. 90.

45 Judgment of 16 December 2008 in Case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, ECLI:EU:C:2008:727, para. 61. Despite the broad interpretation, the CJEU did not consider the activities of an internet search engine as a journalistic activity. See judgment of 13 May 2014 in Case C-131/12 *Google Spain SL,* ECLI:EU:C:2014:317, para. 85. See on that ruling further par. 4.2 below.

46 Judgment of 14 February 2019 in Case C-345/17, *Buivids*, ECLI:EU:C:2019:122, para. 58.

47 Ibid, para. 69.

48 Ibid, para. 68. The CJEU referred the *Satamedia* ruling of the ECtHR which was indeed a further ruling on the same issue as the *Satamedia* ruling of the CJEU. Judgment of the ECtHR of 21 July 2015, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, App. No. 931/13.

accept a greater degree of tolerance regarding the publication of information about them.[49] However, public figures, especially if they did not deliberately choose to be in the public arena, are not without protection.[50] In order to strike a fair balance between privacy and the freedom of expression, the ECtHR also took into account whether the publication contributed to a debate of general interest.[51] This could concern political issues or crimes, but also sporting issues or performing artists.[52] The rumoured marital difficulties of a president, or the financial problems of a famous singer, were not deemed to be matters of general interest.[53] Other elements for the balancing exercise were the subject of the news report; the prior conduct of the person concerned; the method of obtaining the information and the content, form and consequences of the publication.[54] In *Buivids*, the CJEU considered that the possibility for the controller to adopt measures to mitigate the extent of the interference with the right to privacy also had to be taken into account.[55]

4.2 The right to be forgotten

A data subject has the right to require the controller to erase her of his personal data on the basis of one of the grounds listed in article 17(1) GDPR. If the controller made the personal data public, he must take reasonable steps to inform other controllers with whom the data were shared. The right to erasure, also referred to as the right to be forgotten, is not absolute, as follows from article 17(3) GDPR. The right may be limited, *inter alia*, for the protection of freedom of expression and information.[56]

The right to be forgotten has triggered significant debate. An important driver behind the debate was the *Google Spain* ruling of the CJEU in 2014.[57] The case concerned the deletion of a link to a website from the list of results when searching the Internet via Google's search engine on an individual's name. By removing the link from the search results, the information about the person is not really "forgotten", but rather removed

49 See for example judgment of the ECtHR of 8 July 1986, *Lingens v. Austria*, App. No. 9815/82, A-103, para. 42.
50 Judgment of the ECtHR of 24 June 2004, *Von Hannover v. Germany*, App. No. 59320/00, para. 69.
51 Ibid, paras 60-65.
52 Judgment of the ECtHR of 7 February 2012, *Von Hannover v. Germany* (No 2), App. No. 40660/08, para. 109.
53 Ibid.
54 Judgment of the ECtHR of 10 November 2015, *Couderc and Hackette Filipacchi Associés v. France*, App. No. 40454/07, para. 93. This case gives a elaborate overview of the different criteria.
55 Ibid, para. 66.
56 Art. 17(3)(a) GDPR.
57 See Case C-131/12, *Google Spain SL*.

from the "active memory" of the Internet since the website itself remains accessible.[58] Still, such 'dereferencing' also affects the freedom of expression.

In *Google Spain* the Court did not expend many words on the freedom of expression as such.[59] The competing interests referred to by the Court as requiring balancing were: the economic interest of Google; the legitimate interests of internet users potentially interested in having access to the information and the interests of the data subject.[60] However, the interest of the newspaper itself in having wider accessibility of its website was not taken into account. The role of Google as an instrument of freedom of expression in that respect was not directly acknowledged by the Court.[61]

When giving guidance on how to strike the balance, the Court used elements seemingly taken from the case law of the ECtHR discussed above. The point of departure, according to the CJEU, is that the rights of the data subject "as a rule" override the other interests. However, in some circumstances the right of the general public might prevail, which depends on the nature of the information in question; its sensitivity for the data subject's private life and on the interest of the public in having that information which may vary, in particular, according to the role played by the data subject in public life.[62]

The Court was criticised for not giving enough prominence to the freedom of expression in the *Google Spain* ruling. In a second case concerning Google, *GC and others*, AG Szpunar invited the Court to also take into account the freedom of expression of the publisher of the website.[63] The Court eventually gave more prominence to the right to freedom of expression; however, it was still limited to the user of the search engine and not the owner of the webpage, let alone Google itself.[64] Instead of the "legitimate interests" of internet

58 See in relation to the source website, ECtHR 16 July 2013, *Węgrzynowski and Smolczewski v. Poland*, Appl. No. 33846/07. See also S. Wechsler, 'The Right to Remember: The European Convention on Human Rights and the Right to be Forgotten', *Colum. J.L. & Soc. Probs,* Vol. 49, No. 1, 2015, p. 135. Regarding online press archives: ECtHR 28 June 2018, *M.L. and W.W. v. Germany*, App. No. 60798/10 and 65599/10.

59 See for criticism of this point: E. Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12', *HRLR*, Vol. 14, No. 4, 2014, p. 761; S. Kulk and F. Zuiderveen Borgesius, '"Freedom of expression" and "right to be forgotten" cases in the Netherlands after Google Spain', *EDPL,* Vol. 1, No. 2, 2015, p. 113 and C. Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', in B. Hess and C. Mariottini (Eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection*, Farnham/Baden-Baden, Ashgate/Nomos, 2015.

60 Case C-131/12, *Google Spain SL*, para. 81.

61 The Court points at the "important role" played by search engines, but only to underline that its activities constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the website, see paras 80 and 87. See for criticism H. Hijmans, 'Right to have links removed: Evidence of effective data protection', *Maastricht Journal,* Vol., No. 3, 2014, p. 555.

62 Case C-131/12, *Google Spain SL*, at paras 81 and 97. See also on this H. Kranenborg, 'Google and the Right to be Forgotten', *EDPL* Vol. 1, No. 1, 2015, pp. 77-79.

63 Opinion of AG Szpunar of 10 January 2019 in Case C-136/17, *GC and others*, ECLI:EU:C:2019:14, para. 89.

64 Judgment of 24 September 2019 in Case C-136/17 *GC and others,* ECLI:EU:C:2019:773.

users potentially interested in having access to the information, the Court referred to "the right of freedom of information" of internet users potentially interested in accessing the webpage as protected by article 11 of the Charter.[65]

GC and others concerned a request to delist a reference to "sensitive data" (e.g. data concerning health or data revealing sexual orientation).[66] The Court concluded that, having regard to the responsibilities, powers and capabilities of the operator of a search engine, the prohibition to process sensitive data applies to the operator, but via verification *on the basis of a request by the data subject*.[67] This means that the prohibition would not generally obstruct the activity of Google as a search engine operator. The Court considered that the operator of a search engine, when asked to remove a link, must always ascertain whether the inclusion of the link would still be necessary for exercising the right of freedom of information of the internet users potentially interested in accessing that website by means of a search.[68]

In a third Google case, *Google LCC*, the Court recognised that Member States might attach different weight to the freedom of information of internet users when balancing this freedom against the right to privacy and the protection of personal data.[69] According to the Court this is also reflected in article 85 of the GDPR.[70] In that respect, the Court pointed at the consistency mechanism introduced by the GDPR, which should allow the supervisory authorities to find a common solution.[71]

Google LCC concerned the territorial scope of the obligation to dereference. The Court concluded that a search engine operator is not required to carry out a dereferencing on all the versions of its search engine.[72] The dereferencing is, in principle, supposed to be carried out in respect of all the Member States, whereby sufficiently effective measures must be taken to ensure the effective protection of the data subject's fundamental rights.[73]

The *Google LCC* ruling contains an interesting twist at the end. The Court considered that a national supervisory or judicial authority remains competent to weigh up, in the light of national fundamental rights standards, the data subject's rights, on the one hand, and the right to freedom of information, on the other, and to order, where appropriate, the operator of that search engine to carry out a dereferencing concerning all versions of that search engine.[74] The precise implications of this consideration are unclear. How the

65 Ibid, para. 66.
66 See art. 9(1) GDPR for a definition.
67 C-136/17, *GC and others,* para. 47.
68 Ibid, para. 66.
69 Judgment of 24 September 2019 in Case C-507/17, *Google LCC*, ECLI:EU:C:2019:772, para. 67.
70 Ibid, para. 67.
71 Ibid, paras 67-69.
72 Ibid, para. 65.
73 Ibid, paras 66 and 70.
74 Ibid, para. 72.

national balancing exercise can be separated from the European one, keeping in mind that both will relate to the same request for delisting, is unclear. It is equally unclear what value should be given to the considerations of the Court that numerous *third states* do not recognise the right to dereferencing or have a different approach to it and that the outcome of the balancing exercise is likely to vary significantly around the world.[75] In any event, it seems that the uniform application of Union law (i.e. the GDPR) might be compromised if some Member States were to require global delisting, and others did not.[76]

4.3 Data protection and freedom of expression: what level of harmonisation?

According to article 85 GDPR Member States must, by law, reconcile the right to the protection of personal data pursuant to the GDPR with the right to freedom of expression and information.

Arguably, the right to be forgotten and how it relates to the freedom of expression is covered by article 17 GDPR, while the *general* reconciliation of data protection and the freedom of expression is left to the Member States under article 85 GDPR.[77]

Article 85(3) GDPR states that Member States shall notify the provisions of their laws adopted on the basis of that provision to the European Commission. Member States also have to notify, without delay, any subsequent amendment law or amendment affecting them. A study from 2010 showed that there were wide divergences between the Member States.[78] Even more than under the previous *Directive*, the Commission will feel compelled to search for certain coherence in this area in order not to undermine the harmonising effects of the present *Regulation*. The existence of national law also raises questions about the national law applicable in cross-border situations, which can be "particularly sensitive".[79] The issue was recognised by the legislator, which stated in recital 153 of the GDPR that where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply.

---

75 Ibid, paras 59-60.

76 See in this respect judgments of 26 February 2013 in Case C-617/10, *Åkerberg Fransson*, ECLI:EU:C:2013:105, para. 29, and of 26 February 2013 in Case C-399/11, *Melloni*, ECLI:EU:C:2013:107, para. 60 *partially* cited by the CJEU in para. 72 of the *Google LCC* ruling.

77 See in this respect the two orders of the German Federal Constitutional Court of 6 November 2019, at: www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2019/bvg19-083.html and www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2019/bvg19-084.html.

78 Report by D. Korff of 20 January 2010 for the European Commission, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments.*

79 Ibid, pp. 12-13.

5 Enforcement of data protection law in the Union institutions

5.1 Data protection and the Union institutions: Regulation (EU) 2018/1725

The data protection rules for Union institutions and bodies were initially laid down in Regulation (EC) No 45/2001 which also established the EDPS.[80] Since Union institutions and bodies fell outside the scope of the GDPR, Regulation 45/2001 had to be adapted to the GDPR.[81] The new Regulation (EU) 2018/1725 entered into force on 11 December 2018.[82]

While generally aligned with the GDPR, Regulation 2018/1725 displays certain differences, justified by the specific context in which Union institutions and bodies operate. The sections below set out some of those specificities and focus on issues raised in section C of the questionnaire for the present topic.

5.2 The European Data Protection Supervisor

The EDPS is responsible for ensuring that the fundamental rights and freedoms of national persons and, in particular, their right to data protection, are respected by Union institutions and bodies. The EDPS performs *vis-à-vis* the Union institutions and bodies the role of the independent supervisory authority within the meaning of article 8(3) of the Charter and article 16(2) TFEU.

The tasks and powers of the EDPS are generally aligned with those of national supervisory authorities. The rules concerning appointment, performance of duties, and independence have not changed much. This is not surprising: in three cases related to the independence of national data protection authorities, the CJEU considered the EDPS as a benchmark for the independence of supervisory authorities.[83] The EDPS is appointed for a term of five years by common accord of the European Parliament and of the Council,

80 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1. The appointment of the first EDPS (Peter Hustinx) and Assistant EDPS (JoaquínBayo Delgado) took effect only in January 2004.

81 See art. 2(3) GDPR.

82 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

83 See C-518/07, *Commission v. Germany*, ECLI:EU:C:2010:125, C-614/10, *Commission v. Austria*, ECLI:EU:C:2012:631, and C-288/12, *Commission v. Hungary*, ECLI:EU:C:2014:237.

on the basis of a shortlist of at least three candidates drawn up by the Commission following a public call for candidates.

5.3 *Consultative role of the EDPS (legislative consultation)*

Under Regulation 45/2001, the EDPS was tasked already with advising the Commission and other institutions on new legislative proposals and other measures relating to the protection of personal data.[84] The first formal legislative opinion was issued on 22 October 2004.[85] Since then, the awareness of the Commission services grew and with it the number of EDPS opinions, reaching an average of 10-12 opinions and 20-30 formal comments per year.[86]

In line with the GDPR, Regulation 2018/1725 boosted the consultative role of the EDPS, consolidating the practices developed over longer than the past decade.[87] Article 42(1) explicitly requires the Commission to consult the EDPS following the adoption of proposals for a legislative act; of recommendations and of proposals to the Council pursuant to article 218 TFEU (i.e. international agreements) or when preparing delegated or implementing acts with 'an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.

Article 42(2) provides for the possibility in certain cases for the Commission to consult also the EDPB (of which the EDPS is a member). In such cases, the EDPS and the EDPB should coordinate their work with a view to issuing a joint opinion. The EDPS still maintains its role as a privileged advisor to all EU institutions and bodies on data protection issues, while the EDPB's advisory powers are limited to the Commission.[88]

5.4 *The EDPS' approach to complaints*

The right to lodge a complaint with the EDPS is enshrined in article 63 of Regulation 2018/1725. The EDPS must handle the complaint or inform the data subject about the progress or outcome in three months (in line with article 78(2) GDPR).

84 Arts 28, 41 and 46(d) Regulation 45/2001.

85 [2004] OJ C301/4, also available at http://edps.europa.eu/sites/edp/files/publication/04-10-22_financial_interests_en.pdf.

86 See EDPS Annual Reports, http://edps.europa.eu/annual-reports_en.

87 See EDPS Policy Paper of 4 June 2014, http://edps.europa.eu/sites/edp/files/publication/14-06-04_pp_edpsadvisor_en.pdf.

88 See rec. 60, art. 42, 57(1)(g) and 58(3)(c) Regulation 2018/1725, and art. 70 GDPR.

Since the entry into force of Regulation 2018/1725, the EDPS has not yet published an updated general enforcement strategy.[89] However, the main elements of the approach to complaints have been made available on the EDPS website.

Anyone whose personal data are processed by a Union institution or body can complain about that processing.[90] In addition, anyone who is employed by a Union institution or body can complain about breaches of the data protection rules by a Union institution or body, even if they are not personally affected.[91] Anonymous complaints are not handled. Moreover, the EDPS does not deal with complaints which are before a court or that have already been settled by a court, nor with matters that are being examined by the European Ombudsman. At the same time, the admissibility of a complaint is not affected by the fact that another Union institution is examining it, but the EDPS can decide to await the outcome of that body's procedures before starting its own investigation.[92]

In 2018, the EDPS received 298 complaints, an increase of 111% compared to 2017. Of these, 240 complaints were inadmissible (the majority did not concern processing by a Union institution or body) and 23 complaints were closed with a decision. The remaining 58 complaints required in-depth inquiry, an increase of 132% compared to 2017. 38 cases submitted in previous years were still in the inquiry, review or follow-up phase on 31 December 2018.[93]

5.5 *Administrative fines*

Regulation 2018/1725 granted the EDPS the power to impose administrative fines on Union institutions and bodies.[94] During the legislative process the Member States were divided over this issue, which can be explained by the fact that only a minority of them made use of the possibility under article 83(7) GDPR to allow for administrative fines for data protection infringements to be imposed on public authorities. The EDPS supported the introduction of this power mainly because of its deterrent effect.

The sanctions regime for Union institutions and bodies differs in several important aspects from the rules set out in the GDPR. While administrative fines under the GDPR can, as a general rule, be imposed in addition to, or instead of, other corrective measures,[95]

89 For the approach under the old Regulation 45/2001, see EDPS Policy Paper of 13 December 2010, http://edps.europa.eu/sites/edp/files/publication/10-12-13_pp_compliance_en_0.pdf.

90 In addition, the EDPS specifies that a complaint will be investigated only if it concerns a real or potential and not a hypothetical breach of personal data protection rules, and only if it is lodged within two years from the date the data subject became aware of the facts on which the complaint is based.

91 Art. 67 Regulation 2018/1725.

92 See https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

93 www.op.europa.eu/webpub/edps/2018-edps-annual-report/en/, p. 37.

94 Art. 66 Regulation 2018/1725.

95 Art. 83(2) GDPR.

fines under Regulation 2018/1725 are clearly meant as sanctions of last resort, to be imposed only in case of non-compliance with one of the other corrective measures under article 58(2)(d) to (h) and (j).[96]

Moreover, maximum limits for administrative fines under article 66 are significantly lower than those provided for under article 83 GDPR and may not exceed 25,000 euro per infringement in most cases, and up to a total of 250,000 euro per year. Higher fines (up to 50,000 euro per infringement and up to 500,000 euro per year) may only be imposed for infringements of the basic principles for processing, including consent, data subjects' rights, and rules related to international transfers. The total amount of fines imposed for several infringements related to linked or continuing processing operations cannot exceed the amount specified for the gravest infringement. This approach appears justified given that, unlike the GDPR, Regulation 2018/1725 does not apply to operators pursuing gainful activities. Moreover, fines of this order of magnitude, while undoubtedly having deterrent effect, would not risk jeopardising the day-to-day functioning of the Union institution in question. It should be emphasised that the funds collected by imposition of administrative fines will not be linked in any way to the budget of the EDPS, but would form part of the general budget of the Union.[97]

5.6 The data protection officer in Union institutions and bodies: A model for the GDPR

Almost twenty years ago, Regulation (EC) 45/2001 introduced an interesting, if not unique feature, of the data protection framework applicable to Union institutions and bodies: the obligation for all Union institutions and bodies to appoint a data protection officer (hereinafter "DPO").[98]

DPOs were tasked with ensuring the internal application of the Regulation in an independent manner.[99] The first Annual Report of the EDPS presented the DPOs as a key figure for the achievement of effective personal data protection and acknowledged that the DPOs (some of whom were appointed even before the first EDPS and Assistant EDPS were effectively appointed in January 2004) had done "very useful work".[100]

96 Rec. 81 Regulation 2018/1725.

97 Art. 66(7) Regulation 2018/1725.

98 Member States could provide for the appointment of a "data protection officer" already under Directive 95/46/EC, see art. 18(2). However, this possibility was not widely used.

99 The independence of the DPO is understood as preventing them from receiving instructions regarding the exercise of their tasks.

100 EDPS, Annual Report 2004, https://edps.europa.eu/sites/edp/files/publication/annual_report_2004_en.pdf, p. 11.

Over the years, the EDPS provided guidance on the role of the DPO; the type of profile required for a DPO and the resources that should be allocated to the DPO to ensure the good performance of their duties. The latest "position paper" took into account some novelties introduced by Regulation (EU) 2018/1725, e.g. the possibility to appoint a single DPO for more than one Union institution or body. The EDPS considered, in particular, that in order to be able to carry out the assigned tasks and responsibilities, DPOs should be provided with adequate support at material, staff and managerial levels. Performing the role of a DPO on a part-time basis is not excluded (and in fact it is quite common), but in any event the DPO should have sufficient time to fulfil their duties.[101]

The obligation to appoint a DPO was introduced in the GDPR as one of the elements strengthening controllers' and processors' responsibility and accountability, moving away from the rather bureaucratic approach based on notification to or prior-checking by a supervisory authority.[102] Already before the adoption of the GDPR, the Article 29 Working Party argued that the DPO "is a cornerstone of accountability" and that it will continue to be at the heart of the new accountability-based framework as intermediary between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).[103]

The designation of a DPO under the GDPR is mandatory for controllers (and processors) in the public sector (except for courts acting in their judicial capacity) and for those whose activities require regular and systematic monitoring of data subjects on a large scale, or consist of processing on a large scale of "sensitive data" or data related to criminal convictions.[104] The GDPR requires DPOs to be provided with necessary resources and support to maintain their expert knowledge, and to report to top management of the controller or processor.[105]

Beyond supporting the controller or processor internally, thus facilitating compliance with data protection rules, the DPO also act as a contact point for the supervisory authority, and is tasked with cooperating with the authority more generally.[106]

---

101 EDPS, Position Paper of 30 September 2018, https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf.

102 See the Commission Impact Assessment accompanying the proposal for the General Data Protection Regulation, SEC(2012)72/2, p. 51. Designation of a DPO is also mandatory for police and judicial authorities subject to the Law Enforcement Directive (see art. 32). Also in this case, Member States may exempt courts and other independent judicial authorities when acting in their judicial capacities from that obligation. For a discussion of the principle of accountability, C. Docksey, 'Commentary on article 24 GDPR' in: C. Kuner et al, (Eds), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2019.

103 Article 29 Working Party Guidelines on Data Protection Officers (DPOs), WP 243 rev. 01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048, p. 4.

104 Art. 37 GDPR.

105 Art. 38(2) and (3) GDPR.

106 Art. 39(1)(d) and (e) GDPR.

5.7 Data protection rules for EU law enforcement agencies

Chapter IX of Regulation (EU) 2018/1725 lays down the rules applicable to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall under the provisions on judicial cooperation in criminal matters or police cooperation.[107] Operational personal data is the personal data processed when carrying out such activities to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies. Other processing activities are covered by the "normal" rules of the Regulation. Chapter IX was not included in the Commission proposal, but was added during the legislative process at the insistence of the European Parliament. The provisions are based on those of the Law Enforcement Directive, in a way "transposing" it for the EU agencies, providing for one single instrument at Union level.

Since 12 December 2019, the provisions also apply to the processing of operational personal data by the European Union Agency for Criminal Justice Cooperation ("Eurojust").[108] In the future, the Commission will have to review the relevant legal acts governing the processing of operational personal data and may make legislative proposals, in particular with a view to applying Chapter IX to the European Police Office (Europol) and the European Public Prosecutors Office (EPPO).[109]

5.8 Remedies for non-compliance

Non-contractual liability of the Union requires the following elements to be present: actual damage; a causal link between the damage claimed and conduct alleged against the institution; and the illegality of such conduct.[110] Claims for compensation may be brought before the General Court pursuant to article 268 TFEU and article 340(2) TFEU, or concerning relations between the Union and its servants under article 270 TFEU.[111]

The CJEU has accepted liability of Union institutions for breaches of the former Regulation (EC) 45/2001. In *Nanopoulos v. Commission*, confidential information about the applicant was leaked to the press and subsequently included in press articles.[112] It is for the applicant in an action for damages to establish that the conditions for non-contractual liability are satisfied. However, the burden of proof shifts to the institution

107 Art. 2(2) Regulation 2018/1725.

108 Art. 26(1) Regulation 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA [2018] OJ L295/138.

109 Art. 98 Regulation 2018/1725.

110 K. Lenaerts et al, *EU Procedural Law*, Oxford, Oxford University Press, 2014, at 11.01.

111 Previously these cases fell within the exclusive jurisdiction of the Civil Service Tribunal (CST).

112 Judgment of 11 May 2010 in Case F–30/08, *Fotios Nanopoulos v. European Commission*, ECLI:EU:F:2010:43.

when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to what was the true cause, even though it was best placed to do so.[113] As the publication of the applicant's name could only have resulted from an unauthorised disclosure by one of its departments, it was for the Commission to prove that it was not the source of the leak.

In *V v. European Parliament* the applicant challenged the Parliament's decision not to recruit her on grounds of unfitness to be hired. That conclusion was reached based on a medical dossier collected by the European Commission when the same applicant applied for a job there almost two years earlier, and which had been subsequently transmitted to the Parliament.[114] The former Civil Service Tribunal concluded that the transmission was in breach of several provisions of Regulation (EC) 45/2001. The applicant was awarded 5,000 euro for material damages (lost potential earnings). The Court recalled that the annulment of the administration's unlawful act could not constitute full reparation for the non-material damage if that act contains an assessment of the abilities and conduct of the person concerned which is capable of offending them, as was the case here. This particularly serious infringement of Regulation (EC) 45/2001 justified a compensation of 20,000 euro for the non-material damage. More recently, the General Court held *in XI v. Commission* that unnecessary disclosure of sensitive medical data in an administrative decision was sufficient for the Court to find that the applicant had indeed suffered moral damage.[115] The applicant was awarded 2,500 euro in compensation.[116]

In *CN v. Parliament*, a document stating that the applicant was suffering from a life-threatening illness and that his son had a severe disability was published on the Parliament's website in the context of the procedure for handling a petition that the applicant had submitted.[117] Despite the applicant's claims to the contrary, the General Court considered that he had given his express consent to the processing of his personal data, even sensitive data, by the Parliament, including their publication on the internet. The applicant's claims with regard to non-material damage were rejected on the ground that he 'merely claimed' that the Parliament's dismissive and dilatory attitude hurt him deeply and caused him considerable stress, without providing any evidence.[118]

In *Oikonomopoulos v. Commission* the applicant claimed 2 million euro in damages suffered as a result of infringements of the Regulation by the Commission and OLAF, including reputational damage and loss of income due to the fact that he had to cease his

113 Judgment of 8 July 2008 in Case T-48/05, *Franchet and Byk v. European Commission*, ECLI:EU:T:2008:257, para. 183 and Case F–30/08, *FotiosNanopoulos v. Commission*, para. 161.

114 Judgment of 5 July 2011 in Case F-46/09, *V and EDPS v. European Parliament*, ECLI:EU:F:2011:101.

115 Judgment of 12 September 2019 in Case T-528/18, *XI v. European Commission*, ECLI:EU:T:2019:594.

116 Ibid, paras 75-77. The Commission's appeal against the General Court's ruling is currently pending.

117 Judgment of 3 December 2015 in Case T-343/13, *CN v. European Parliament*, ECLI:EU:T:2015:926.

118 Ibid, para. 121.

professional activity. Even though the Court found an infringement of Regulation (EC) 45/2001, it held that the applicant has not demonstrated the existence of any causal link between that infringement and the damage complained of, and therefore his claim for damages was dismissed as unfounded.[119]

5.9 Cooperation of supervisory authorities with other regulators

The EDPS has long drawn attention to synergies between data protection, consumer protection and competition policy.[120] Increased cooperation between competent authorities could help to deal with challenges posed by the digital economy more effectively.

In 2016, the EDPS launched the Digital Clearinghouse in order to facilitate cooperation and information exchange between regulators and enforcement agencies from across the three areas. The scope of the meetings was later expanded to include electoral regulators, in order to discuss the impact of online manipulation on free and fair elections and the democratic process. From 2019, the Digital Clearinghouse is jointly hosted by the Research Centre in Information, Law and Society (CRIDS) at the University of Namur, the Tilburg Institute for Law, Technology, and Society (TILT) at Tilburg University, and the European Policy Centre (EPC) in Brussels.[121] The emphasis was on the challenges of regulating non-monetary price services and enforcement *vis-à-vis* big tech companies.[122]

6 Data protection and national security

6.1 '…national security remains the sole responsibility of each Member State'

Article 4 TEU combines several elements fundamental to the Union legal order. The first paragraph lays down the principle of conferral: competences not conferred upon the Union remain with the Member States. The second paragraph determines that the Union shall

119 Judgment of 20 July 2016 in Case T-483/13, *Athanassios Oikonomopoulos v. Commission*, ECLI:EU:T:2016:421, para. 247.

120 See EDPS Preliminary Opinion of March 2014, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf and EDPS Opinion of September 2016 on coherent enforcement of fundamental rights in the age of Big Data, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

121 See https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

122 See EDPS Report of 2019, 'Leading by Example EDPS 2015-2019', www.edps.europa.eu/sites/edp/files/publication/edps_2015-2019_en.pdf, p. 23.

respect the equality of Member States before the Treaties as well as their national identities. The second paragraph continues by stating that the Union shall respect the essential State functions of the Member States, which includes ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. Finally, it is added: "[i]n particular national security remains the sole responsibility of each Member State". The third paragraph of article 4 lays down the principle of sincere cooperation: the Union and the Member States shall assist each other in carrying out tasks which flow from the Treaties.

Squeezed between the principles of conferral and sincere cooperation, the precise meaning of the part listing the different elements concerning national identities and essential State functions in article 4(2) is not self-evident.[123] Directly following the principle of conferral, these references could be seen as indicating certain areas that remain the competence of the Member States and are therefore excluded from Union competence. However, given that they are directly followed by the principle of sincere cooperation, paragraph two could also be considered as listing national particularities that have to be *respected* by the Union when exercising its competences.

Adopting the latter interpretation, matters relating to national identities and essential State functions are not as such excluded from the scope of Union law but must be taken into account in the application of Union law. The wording used in article 4(2) ("shall respect") seems to support this latter interpretation. However, the last sentence on (in particular) national security rather supports the first interpretation.[124]

Member States have relied on article 4(2) TEU to argue that certain situations were indeed as such *excluded* from the scope of Union law. In *ZZ* the Court stated that the mere fact that a decision concerns State security cannot result in Union law being inapplicable.[125] In her Opinion in the *Achbita* case, Advocate General Kokott stated that the European Union's obligation under article 4(2) TEU requires that the *application* of Union law must not adversely affect the national identities of the Member States.[126]

If not considered as excluded as such from the scope of Union law, the question rises as to how far the Court can go in assessing the lawfulness of national measures in these areas. Should it limit itself to verifying whether the situation relied upon genuinely qualifies as a national matter mentioned in article 4(2) TEU and leave it at that? Arguably, this

123 See art. 4(2) TEU; also G. Di Federico, 'The Potential of Article 4(2) TEU in the Solution of Constitutional Clashes Based on Alleged Violations of National Identity and the Quest for Adequate (Judicial) Standards', *EPL*, Vol. 25, No. 3, 2019, pp. 347-380 and S. Sule, 'National Security and EU law restraints on Intelligence Activities', in J. H. Dietrich and S. Sule (Eds), *Intelligence Law and Policies in Europe*, Munich, Beck, 2019, pp. 335-387.

124 To be noted that reference is made to the sole *responsibility* and not to the sole *competence* of the Member States.

125 Judgment of 4 June 2013 in Case C-300/11, *ZZ*, ECLI:EU:C:2013:363, para. 38.

126 Opinion of 31 May 2016 in Case C-157/15, *Achbita*, ECLI:EU:C:2016:382, para. 32 (emphasis in original).

would then still amount to an exclusion assessment. Or should the Court treat article 4(2) TEU rather as *derogation* from Union law, which should be interpreted strictly, and also includes an assessment of the proportionality of the national measure?

So far, the Court treated article 4(2) TEU mostly as a possible ground for *derogation* from Union law, so applying a strict interpretation and assessing the proportionality of the national measure. Admittedly, this might also be due to the fact that article 4(2) TEU was almost always invoked in conjunction with grounds for derogations which were explicitly provided for elsewhere in Union law (e.g. in the Treaty provisions on free movement, or in secondary legislation). In these cases, considerations relating to article 4(2) TEU fed into the assessment of whether the derogation provided for elsewhere could be relied upon. Article 4(2) TEU helped to qualify the objective pursued by the derogation.[127]

The cases concerning specifically national security were indeed all based on other Union law provisions as well, such as article 346(1) TFEU which itself includes a necessity requirement.[128] This justified a review by the Court also going into the proportionality of the measure at issue.[129]

It has not yet been established whether in relation to national security, article 4(2) TEU could be invoked independently from any other provision in Union law and, if so, whether it will be treated as a ground for derogation; or, with a view to the explicit language in the last sentence of article 4(2) TEU, whether the assessment would rather be limited to verifying whether the situation relied upon genuinely qualifies as a matter of national security.

In *Correia Moreira*, which did not concern national security, the Court seemed to imply that once a matter is harmonised by Union law, and no exclusion or derogation is foreseen for national specificities, article 4(2) TEU cannot be relied upon in order not to apply those rules.[130]

---

127 E.g. the Court has qualified as belonging to the national identity: the protection of the official language or languages of the Member States, the status of a Member State as a Republic and the division of competences within a Member States, including internal reorganisations of powers. See resp. judgment of 12 May 2011 in Case C-391/09, *Runevič-Vardyn*, ECLI:EU:C:2011:291, para. 86; judgment of 16 April 2013 in Case C-202/11, *Anton Las*, ECLI:EU:C:2013:239, para. 26/27; judgment of 22 December 2010 in Case C-208/09, *Sayn-Wittgenstein*, ECLI:EU:C:2010:806, para. 92 and judgment of 21 December 2016 in Case C-51/15, *Remondis*, ECLI:EU:C:2016:985, para. 40. See also judgment of 2 June 2016 in Case C-438/14, *Bogendorff von Wolffersdorff*, ECLI:EU:C:2016:401, para. 64.

128 See for example judgment of 20 March 2018 in Case C-187/16, *Commission v. Austria*, ECLI:EU:C:2018:194, para. 78.

129 See art. 346(1)(a) and (b) TFEU. Only art. 346(1)(b) contains a reference to the necessity of the measure, but the Court considered the same requirement to apply to art. 346(1)(a) TFEU. See *Commission v. Austria*, ibid, para. 78. See for example *Sayn-Wittgenstein*, ibid, paras 91-93. See also the Opinion of AG Kokott in Case C-157/15, *Achbita*, para. 125.

130 See judgment of 13 June 2019 in Case C-317/18, *Correia Moreira*, ECLI:EU:C:2019:499, para. 61 and 62.

6.2 National security in secondary EU data protection legislation: Exclusion and/or derogation?

In Union data protection legislation, national security can be found in exclusionary clauses as well as in derogation clauses.[131] The former Directive (EC) 95/46 did not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law […] and in any case to processing operations concerning public security, defence, State security […] and the activities of the State in areas of criminal law'.[132] On the other hand, article 13 of Directive (EC) 95/46 allowed Member States to adopt legislative measures to *restrict* the scope of rights and obligations in the Directive when it constituted a necessary measure to safeguard, *inter alia*, national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences.[133] Similar provisions can be found in article 2(2)(a) and article 23 GDPR and in articles 1(3) and 15(1) of the ePrivacy Directive.[134]

The CJEU was asked about the interplay of these provisions in several cases in which commercially collected data were used by public authorities for law enforcement purposes.[135] After the invalidation of the notorious Data Retention Directive in *Digital Rights Ireland,*[136] several Member States kept in place national data retention legislation requiring telecoms providers to retain the metadata of customers for a certain period in order for the data to be available for access by law enforcement authorities. The Court was asked whether the national legislation at issue actually fell within the scope of Union law. The Court had to clarify the relationship between the exclusion clause of article 1(3), and the derogation clause of article 15(1) of the ePrivacy Directive. This led to the seminal *Tele2/Watson* ruling.[137]

Regarding article 1(3), the Court considered that that provision excluded from the scope of the ePrivacy Directive 'activities of the State' in specified fields, including in areas

131 For the sake of simplicity national security, State security and public security are used interchangeably, although the notions do not necessarily have the exact same meaning.

132 Art. 3(2) Directive 95/46/EC.

133 Art. 13(1)(a)-(d) Directive 95/46/EC.

134 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

135 See for the first time, judgment of 30 May 2006 in Cases C-317/04 and C-318/04, *European Parliament v. Council and Commission*, ECLI:EU:C:2006:346.

136 Judgment of 8 April 2014 in Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, para. 54 onwards, in particular paras 60-62 regarding Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] L105/54.

137 Judgment of 21 December 2016 in Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson et al*, ECLI:EU:C:2016:970.

of criminal law and in the areas of public security, defence and State security.[138] The Court underlined that the ePrivacy Directive regulated the activities of telecom providers.[139] When considering article 15(1) the Court admitted that the legislative measures referred to therein also concerned activities characteristic of States or State authorities, which are unrelated to fields in which individuals are active and that the provision listed the same objectives as article 1(3).[140] However, according to the Court, excluding the national measures referred to in article 15(1) from the scope of the ePrivacy Directive would deprive article 15(1) of any purpose.[141] According to the Court, article 15(1) actually presupposed that such measures fell within the scope of the Directive. The Court added that the national measures referred to in article 15(1) in fact governed the activity of telecom providers.[142] The retention obligation necessarily invoked the processing, by the telecom providers, of personal data.[143]

The Court went even further by including in the scope of the Directive also national legislative measures that regulated *access* of the national authorities to the data retained by telecom providers (which arguably qualifies as a State activity).[144] This was due to article 5 of the ePrivacy Directive which requires that the confidentiality of communications and related traffic data has to be ensured, which, as the Court considered, had to be respected by any person other than the user, whether private persons or bodies or State bodies.[145] In a later case, *Ministerio Fiscal*, the Court considered that national rules on access for law enforcement purposes fell within the scope of the ePrivacy Directive, regardless of whether the data at issue was stored by the company on the basis of a national data retention law, or simply retained for the normal commercial purposes of the operator.[146]

As a consequence of the above interpretation the Court considered itself competent to formulate conditions for national data retention measures, including for access to such retained data. These conditions were the reason why the *Tele2/Watson* ruling triggered extensive debates. The Court rejected the idea of *generalised* data retention (i.e. retention of all metadata of all users) as opposed to *targeted* retention and formulated several strict

138 Ibid, para. 69. Arguably, the Court went beyond the wording of the provision, which only referred to state activities in relation to criminal law. In the case *Puškar*, the Court considered that the exclusion clause must be interpreted strictly, judgment of 27 September 2017 in Case C-73/16, *Peter Puškar*, ECLI:EU:C:2017:725, para. 38.

139 With reference to art. 3 of Directive 2002/58, see Cases C-203/15 and C-698/15, *Tele2/Watson*, para. 70.

140 Cases C-203/15 and C-698/15, *Tele2/Watson*, para. 72.

141 Ibid, para. 73. See to that effect already the Opinion of AG Bot of 14 October 2008 in Case C-301/06, *Ireland v. European Parliament and Council*, ECLI:EU:C:2008:558, para. 129.

142 Cases C-203/15 and C-698/15, *Tele2/Watson*, para. 74.

143 Ibid, para. 75.

144 Ibid, para. 76.

145 Ibid, para. 77.

146 Judgment of 2 October 2018 in Case C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788, para. 37.

conditions to which access should be subject, including prior authorisation by a court or an independent authority.[147]

In subsequent French, Belgian and British cases, the question was raised whether the reasoning in *Tele2/Watson* on the scope of the ePrivacy Directive would be the same if the national measure at issue did not concern law enforcement but *national security*. According to the Member States involved, article 4(2) TEU supported a reasoning that would exclude from the scope of the Directive activities of the State for the purpose of national security as well as the related activities of the telecom providers. As a subsidiary point, it was argued that if these national measures were considered to fall within the scope of the ePrivacy Directive, generalised retention should be possible for the purpose of national security and the conditions for access by security authorities to data held by telecom operators should not be as strict as in *Tele2/Watson*. AG Campos Sánchez-Bordona proposed that the Court decide that when the cooperation of private parties, on whom certain obligations are imposed, is required, the activities of public authorities aimed at safeguarding national security come within the scope of Union law.[148] He furthermore suggested upholding the criteria as developed in *Tele2/Watson*, albeit with a nuance regarding the requirement that the retention of data should be targeted.[149]

The outcome of these cases, which were still pending at the time of writing, will be of great importance for the Member States who fear Union interference with their national security measures which, as they argue, fall within the sole competence of the Member States. It remains to be seen what meaning the Court will give to the last sentence of article 4(2) TEU when interpreting the exclusion and derogation clauses of the ePrivacy Directive and also what effect it might have on the possible proportionality assessment it makes.

6.3 And the national security of third countries?

National security also plays an important role in the transfer of personal data to third countries. When assessing whether a third country ensures an adequate level of protection, the Commission must not only look at any relevant data protection law in that third state, it has to assess the legal situation of that country as a whole. Article 45(2)(a) GDPR requires the Commission to take into account, *inter alia*, the rule of law, respect for human rights and relevant legislation concerning public security, defence and national security.

147 See Cases C-203/15 and C-698/15, *Tele2/Watson*, resp. paras 104-112 and paras 117-123.

148 Opinions of AG Campos Sánchez-Bordona of 15 January 2020 in Cases C-623/17 *Privacy International*, ECLI:EU:C:2020:5, para. 34 and C-511/18 and C-512/18 *La Quadrature du Net*, ECLI:EU:C:2020:6, para. 85.

149 Opinions of AG Campos Sánchez-Bordona of 15 January 2020 in Case C-520/18, *Ordre des barreaux francophones et germanophone*, ECLI:EU:C:2020:7, paras 72-107.

The content of article 45(2) GDPR is largely inspired by the *Schrems* ruling of the CJEU of 2015. In *Schrems* the Court made clear that the Commission cannot decide positively on the adequacy of the level of data protection in a third country if the law on national security permits security authorities to have access on a generalised basis to the content of electronic communications data transferred to that country and if it does not provide for any possibility to pursue legal remedies to invoke rights in relation to the transferred data once acquired by those authorities.[150] This would not respect the essence of the rights contained in articles 7 and 47 of the Charter.

In the negotiations on the EU-U.S. Privacy Shield, the pending annulment action before the General Court and in the second *Schrems* case before the CJEU, the U.S. government argued that since national security falls outside the scope of Union law, the national legislation of third countries in that area should also be left out of the assessment of whether the third country ensures an adequate level of protection.[151] Given the first *Schrems* ruling it is clear that this argument cannot hold.[152]

It should be noted that article 4(2) TEU refers to the national security *of the Member States* and not that of third countries. Moreover, when adopting an adequacy decision, the Commission takes responsibility for the fact that the data may be transferred to the third country (provided all other conditions of the GDPR are met). Since the personal data must remain subject to a high level of protection if it is transferred to a third country,[153] the assessment necessarily includes an analysis of the general legal situation in the third country, including national security.

As follows from article 2 TEU the Union is founded on the values of respect for the rule of law and for human rights. As the CJEU has stated in the Opinion on the accession of the EU to the ECHR, the Union is based on the fundamental premise that each Member State shares with all the other Member States a set of common values which implies and justifies the existence of mutual trust between the Member States that those values will be recognised.[154] Against this background it is justified to leave certain matters to the Member State without further assessment, while for third countries a further assessment as regards those values still remains necessary.

150 Judgment of 6 October 2015 in Case C-362/14, *Schrems*, ECLI:EU:C:2015:650, paras 94 and 95.

151 Case T-738/16, *La Quadrature du Net/Commission,* ECLI:EU:T:2018:520 and Case C-311/18, *Facebook Ireland and Schrems*. Case T-738/16 was suspended awaiting the outcome of Case C-311/18.

152 See also the Opinion of AG Saugmandsgard Øe of 19 December 2019 in Case C-311/18, *Facebook Ireland and Schrems*, ECLI:EU:C:2019:1145, paras 100-110.

153 See Case C-362/14, *Schrems*, para. 72 and Opinion A-1/15 of 26 July 2017, ECLI:EU:C:2016:656, para. 134. See on this opinion C. Kuner 'International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, *EU-Canada PNR*', *CMLR,* Vol. 55, No. 3, 2018, p. 857-882.

154 Opinion A-2/13 of 18 December 2014, ECLI:EU:C:2014:2454, para. 168.

National Reports

Austria

Hans Kristoferitsch[*]

A Setting the Scene – Weichenstellung

Frage 1

1.1 Auswahl nationaler Rechtsinstrumente zur Umsetzung der DSGVO

Die zur Ergänzung und Durchführung der DSGVO und zur Umsetzung der RL (EU) 2016/680 erforderlichen legistischen Schritte wurden in Österreich im ***Datenschutz-Anpassungsgesetz 2018***[1] gesetzt. Durch dieses wurde das österreichische Datenschutzgesetz („**DSG**") grundlegend umgestaltet. So wurden im DSG sämtliche aufgrund der DSGVO auf nationaler Ebene erforderlich gewordenen Regelungen etwa im Bereich der Organisation der Aufsichtsbehörde, des Verfahrensrechts, der Verhängung von Strafen sowie ausgewählte weitere Regelungen wie etwa in Bezug auf Bildverarbeitung getroffen; im 3. Hauptstück des DSG erfolgte die Umsetzung der RL 2016/680.

Die DSGVO machte darüber hinaus aber auch Änderungen zahlreicher weiterer Gesetze erforderlich. Dies erfolgte in erster Linie im Rahmen des

1. Materien-Datenschutz-Anpassungsgesetzes 2018[2] und des

2. Materien-Datenschutz-Anpassungsgesetzes 2018[3], durch welche über 100 sonstige Gesetze angepasst wurden.

Kurz vor Inkrafttreten der DSGVO wurde vom österreichischen Gesetzgeber schließlich mit dem ***Datenschutz-Deregulierungsgesetz 2018***[4] der (umstrittene) Versuch unternommen, in Bezug auf die Strafbestimmungen (vgl. dazu noch Frage 11), die *Befugnisse von Datenschutzorganisationen* (siehe Frage 13) und das *Medienprivileg* (siehe Frage 8) einige als zu streng empfundene Bestimmungen der DSGVO zu relativieren bzw. der nationalen Aufsichtsbehörde interpretatorische Leitlinien an die Hand zu geben.

---

* Cerha Hempel Attorneys at law, Vienna, Partner. Der Autor dankt Agnes Balthasar-Wach für ihre wertvolle Unterstützung bei den Arbeiten zu diesem Beitrag.

1 BGBl. I Nr. 120/2017.

2 BGBl. I Nr. 32/2018.

3 BGBl. I Nr. 37/2018.

4 BGBl. I Nr. 24/2018.

1.2 Öffnungsklauseln – Art. 6 Abs. 1 lit. c, Art. 23, Art. 86-90 DSGVO

Zentrale Maxime des österreichischen Gesetzgebers bei der Ausgestaltung der in den Öffnungsklauseln der DSGVO enthaltenen Flexibilität war es, ein „*gold plating*" zu verhindern, also keine strengeren Regelungen vorzusehen als unionsrechtlich vorgegeben.

Der Umgang des nationalen Gesetzgebers mit den Öffnungsklauseln kann im Folgenden nur anhand einiger ausgewählter Beispiele illustriert werden:

1.2.1 Art. 6 Abs. 1 lit. c iVm. Abs. 2 DSGVO:

Vom österreichischen Gesetzgeber wurden gestützt auf die Öffnungsklausel in Art. 6 Abs. 1 lit c iVm Abs. 2 DSGVO die zuvor im DSG 2000 geregelten *besonderen Verwendungszwecke* von Daten (zB. §§ 47 bis 48a DSG 2000[5]) und *Regelungen zur Videoüberwachung* (§§ 50a bis 50e DSG 2000) ins neue DSG übernommen; ebenso wurden die Regelungen zur Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke (§ 7 DSG) auf Art. 6 Abs. 2 DSGVO gestützt; gleiches gilt für die Verarbeitung personenbezogener Daten im Katastrophenfall (§ 10 DSG) sowie die Regelungen in Bezug auf Bildverarbeitung (§ 12, § 13 DSG).[6]

Die Mehrzahl der auf Art. 6 Abs. 2 DSGVO gestützten gesetzlichen Regelungen findet sich allerdings nicht im DSG, sondern in den erwähnten, aufgrund der DSGVO angepassten *Materiengesetzen* (vgl. als eines von zahlreichen möglichen Beispielen § 31a Bauarbeiter-Urlaubs- und Abfertigungsgesetz).[7]

1.2.2 Art. 23 DSGVO:

Das Datenschutz-Deregulierungsgesetz führte auf Grundlage von Art. 23 DSGVO „*im Sinne eines Interessensausgleichs*" in § 4 Abs. 5 DSG eine Beschränkung des Auskunftsrechts ein. Demnach besteht das Recht auf Auskunft gegenüber hoheitlich tätigen Verantwortlichen dann nicht, wenn die Erteilung der Auskunft die Erfüllung von dem Verantwortlichen gesetzlich übertragenen Aufgaben gefährden würde. Begründet wurde dies damit, dass sich für „zuständige Behörden" Beschränkungen schon aus dem 3. Hauptstück des DSG sowie aus einschlägigen Materiengesetzen (zB. SPG) ergeben, für

---

5 Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen, Publizistische Tätigkeit, Verwendung von Daten im Katastrophenfall.

6 Im Zusammenhang mit § 12 DSG war allerdings schon im Vorfeld (ähnlich wie in Deutschland) fraglich, ob durch die DSGVO insoweit überhaupt ein Gestaltungsspielraum für den nationalen Gesetzgeber eröffnet wurde. Vgl. dazu zB. Müllner/Wieser, §§ 12 f DSG – Kein Spielraum für Beharrlichkeit, jusIT 2018, 72. Hierzu hat das Bundesverwaltungsgericht nun mittlerweile in zwei (nicht rechtskräftigen) Entscheidungen die Gültigkeit von § 12 und § 13 DSG im Lichte der DSGVO in Zweifel gezogen. Es hat entschieden, dass für § 13 DSG und § 12 Abs. 4 Z 1 DSG keine Öffnungsklausel besteht und diese Bestimmungen daher nicht anzuwenden sind (BVwG 20.11.2019, W256 2214855-1; BVwG 25.11.2019, W211 2210458-1).

7 ERlRV, 65 Blg XXVI. GP (Materien-Datenschutz-Anpassungsgesetz 2018), 33.

den Bereich der allgemeinen Verwaltung im Anwendungsbereich der DSGVO jedoch keine derartigen Beschränkungen vorgesehen waren.

In den Materien-Datenschutz-Anpassungsgesetzen finden sich zahlreiche weitere gestützt auf Art. 23 DSGVO erlassene Regelungen. Dies bspw. im Zusammenhang mit

- der Beschränkung der *Informationspflichten* (zB. § 2b Abs. 3 Gesundheits- und Krankenpflegegesetz, § 2b Abs. 3 Sanitätergesetz, § 2a Abs. 3 Zahnärztegesetz, § 19 Abs. 3 Fortpflanzungsmedizingesetz, § 3b Abs. 2 Ärztegesetz, § 8 Abs. 6 Suchtmittelgesetz, § 48e Bundesabgabenordnung);
- der Beschränkung des *Auskunftsrechts* (zB. § 21 Abs. 6 Finanzmarkt-Geldwäschegesetz, § 104c Bundeshaushaltsgesetz, § 7 Abs. 11 IVF-Fonds-Gesetz, § 11 Abs. 4 Wettbewerbsgesetz, § 48f Bundesabgabenordnung);
- der Beschränkung des Rechts auf *Berichtigung* (zB. § 104d Bundeshaushaltsgesetz, § 7 Abs. 11 IVF-Fonds-Gesetz, § 280b Abs. 5-8 Beamten-Dienstrechtsgesetz, § 48g Bundesabgabenordnung);
- der Beschränkung des Rechts auf *Löschung* (zB. § 104e Bundeshaushaltsgesetz, § 280b Abs. 6 Beamten-Dienstrechtsgesetz);
- der Beschränkung des Rechts auf *Einschränkung der Verarbeitung* (zB. § 2b Abs. 3 Gesundheits- und Krankenpflegegesetz, § 2b Abs. 3 Kardiotechnikergesetz, § 19 Abs. 3 Fortpflanzungsmedizingesetz, § 3b Abs. 2 Ärztegesetz, § 8 Abs. 6 Suchtmittelgesetz);
- der Beschränkung des *Widerspruchsrechts* (zB. § 22f Finanzmarktaufsichtsbehördengesetz, § 2b Abs. 3 Gesundheits- und Krankenpflegegesetz, § 2a Abs. 3 Zahnärztegesetz, § 9 Abs. 4 Gesundheitsberuferegister-Gesetz, § 11 Abs. 5 Wettbewerbsgesetz).

1.2.3 Art. 86 bis 90 DSGVO:

Der österreichische Gesetzgeber hat von diesen Öffnungsklauseln nur begrenzt Gebrauch gemacht:

- Hinsichtlich der Öffnungsklausel des Art. 86 DSGVO wurde (anders als in Deutschland) bislang kein Gesetz erlassen, welches den Zugang zu amtlichen Informationen und den Schutz personenbezogener Daten ausbalanciert.[8] Die Verabschiedung eines solchen Informationsfreiheitsgesetztes („IFG") wird in Österreich allerdings schon längere Zeit diskutiert; zuletzt wurde die Behandlung eines Anfang 2019 eingebrachten Initiativantrags am 1.7.2019 vertagt.
- Von der Öffnungsklausel des Art. 87 DSGVO wurde ua. im Bereich Wissenschaft und Forschung Gebrauch gemacht (vgl. Datenschutzanpassungsgesetz 2018 – Wissenschaft und Forschung[9] hinsichtlich der Zulässigkeit der Verarbeitung nationaler Kennziffern,

8 Öhlböck in Knyrim, DatKomm Art. 86 DSGVO Rz. 8.

9 BGBl. I Nr. 31/2018.

wie ua. Stammzahl gemäß § 2 Z 8 des E-Government-Gesetz, § 2d Abs. 2 und 9, § 2e, § 2k Abs.3 und § 21 Abs. 2 Forschungsorganisationsgesetz; § 43 Abs. 5 Hochschülerinnen- und Hochschülerschaftsgesetz.[10]

- Nach dem Datenschutz-Anpassungsgesetz war zunächst vorgesehen, das Arbeitsverfassungsgesetz (ArbVG), soweit es die Verarbeitung personenbezogener Daten regelt, als Vorschrift iSd. Art. 88 DSGVO zu definieren. Dieser Verweis, durch welchen die im ArbVG enthaltenen Bestimmungen des kollektiven Arbeitsrechts (ua. Erfordernis einer Betriebsvereinbarung für bestimmte Datenverarbeitungstätigkeiten) als Regelungen zur Verarbeitung personenbezogener Daten im Beschäftigungskontext iSd. Art. 88 DSGVO positiviert worden wären, wurde jedoch im Zuge des Datenschutz-Deregulierungsgesetzes wieder gestrichen. Von der Öffnungsklausel des Art. 88 DSGVO wurde daher im österreichischen Recht nur sehr punktuell Gebrauch gemacht (vgl zB. § 280a Beamten-Dienstrechtsgesetz).
- Hingegen wurde die Öffnungsklausel des Art. 89 DSGVO im Rahmen der Materien-Datenschutz-Anpassungsgesetze sehr häufig genützt (dies bspw. in Zusammenhang mit § 2b Abs. 4 Gesundheits- und Krankenpflegegesetz, § 61d Abs. 5 Hebammengesetz, §3a Abs. 4 Medizinische Assistenzberufe-Gesetz, § 16b Abs. 5 Meldegesetz, § 13a Abs. 2 Strafregistergesetz).
- Von der Öffnungsklausel des Art. 90 DSGVO wurde kein Gebrauch gemacht und wurde daher auch keine Mitteilung an die Europäische Kommission erstattet.[11]

1.3 Aufsichtsbehörde

Die österreichische Datenschutzbehörde („DSB") ist nationale Aufsichtsbehörde iSd. Art. 51 DSGVO (siehe im Detail Frage 9) und daher zur Aufsicht über die zur Umsetzung der DSGVO in Österreich ergangenen Bestimmungen zuständig, soweit sich diese im DSG finden; das von der DSB anzuwendende Verfahrensrecht ist das Allgemeine Verwaltungsverfahrensgesetz („AVG")[12] sowie das Verwaltungsstrafgesetz („VStG")[13]. Für die Vollziehung der in sonstigen Materiengesetzen enthaltenen Bestimmungen sind die jeweils sachlich und örtlich zuständigen Behörden zuständig.

10 Öhlböck in Knyrim, DatKomm Art. 87 DSGVO Rz. 2.

11 Pollirer in Knyrim, DatKomm Art. 90 DSGVO Rz. 27; ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en. Hinweis: Die Fundstellen der Online-Quellen wurden zuletzt am 1.2.2020 besucht.

12 StF: BGBl. Nr. 51/1991 (BGBl. I Nr. 58/2018).

13 StF: BGBl. Nr. 52/1991 idF BGBl. I Nr. 194/1999.

Frage 2

Schon vor Inkrafttreten der GRC unterschied die österreichische Rechtsordnung zwischen dem *Grundrecht auf Datenschutz* und dem *Grundrecht auf Achtung des Privat- und Familienlebens*. Letzteres wird ausdrücklich durch die in Österreich im Verfassungsrang stehende Bestimmung des Art. 8 EMRK sowie verschiedene Bestimmungen des Staatsgrundgesetzes 1867 (Art. 9 – Hausrecht, Art. 10 – Briefgeheimnis, Art. 11 – Fernmeldegeheimnis) gewährleistet. Das ebenso in Österreich verfassungsrechtlich verankerte Grundrecht auf Datenschutz ist demgegenüber wesentlich jünger (das als „Jedermannsrecht" ausgestaltete *Grundrecht auf Datenschutz* in § 1 DSG[14] wurde 1978 eingeführt; der Schutzbereich umfasst dabei auch juristische Personen).

Vor diesem innerstaatlichen Hintergrund ergibt sich, dass auch in der Entscheidungspraxis der Behörden und Gerichte zwischen diesen unterschiedlichen Grundrechten differenziert wurde und daher bei einer Bezugnahme auf Art. 8 GRC oder § 1 DSG nicht automatisch auch Art. 7 GRC oder Art. 8 EMRK mitangeführt wird.[15]

Zumal in bislang zu Art. 8 GRC ergangenen Entscheidungen österreichischer Gerichte häufig festgehalten wurde, dass Art. 8 GRC keinen über die Verfassungsbestimmung des § 1 DSG hinausgehenden Schutzgehalt habe,[16] hat Art. 8 GRC bislang keinen maßgeblichen Einfluss auf die Interpretation des nationalen Rechts entfaltet. Aufgrund des schon zuvor in Bezug auf das Grundrecht auf Datenschutz in Österreich gegebenen hohen Schutzstandards führte die GRC nicht zur Änderung bestehender Rechtsprechungslinien.[17]

B Die Annahme von materiell-rechtlichen DSGVO-Vorschriften in der nationalen Rechtsordnung

Frage 3

3.1 DSB

Soweit ersichtlich bestehen in Österreich keine Besonderheiten, was die Interpretation der in Art. 5 DSGVO geregelten Grundsätze der Datenverarbeitung durch Verantwortliche betrifft. Hingegen hat sich die DSB bereits in einer Reihe von Entscheidungen mit diesen Grundsätzen befasst. Nachstehend werden beispielhaft einige dieser Entscheidungen

14 StF: BGBl. Nr. 565/1978.

15 ZB. DSB 7.3.2019, DSB-D130.033/0003-DSB/2019 (rechtskräftig); DSB 18.1.2013, K121.876/0003-DSK/2013; DSB 13.9.2018, DSB-D123.070/0005-DSB/2018 (rechtskräftig).

16 VfGH 29.9.2012, B 54/12 ua. und nachfolgend zB. VwGH 27.9.2013, 2012/05/0213.

17 Vgl zB. OGH 14.9.2011, 6Ob63/11z; OGH 24.11.2011, 6Ob64/11x.

wiedergegeben (thematisch nach Bildverarbeitung sowie Pflichten des Verantwortlichen gegliedert):

Bildverarbeitung:
Eine wesentliche Rolle spielten die Grundsätze der Verarbeitungstätigkeit in den Entscheidungen der DSB zu *Dash-Cams*. Die DSB stellte dabei einen Verstoß gegen *Art. 5 Abs. 1 lit. a und c* iVm. Art. 6 Abs. 1 DSGVO fest, da die vom Aufnahmebereich der Dash-Cams erfassten Verkehrsteilnehmer insbesondere dann, wenn kein Unfallgeschehen vorliegt, vernünftigerweise nicht damit rechnen müssen, aufgenommen zu werden und verhängte eine Verwaltungsstrafe iHv. EUR 220,-.[18]

Im Rahmen eines Konsultationsverfahrens gemäß Art. 36 DSGVO sprach die DSB in einer Empfehlung aus, dass eine beabsichtigte Aufnahme und kurzzeitige Speicherung von Videos mittels an der Frontscheibe eines *Kfz* angebrachter *Videokamera* nicht durchgeführt werden möge. Dadurch, dass auch das Drücken eines Notfall-Knopfes eine Speicherung der Bilddaten auslöst, sei keine Beschränkung auf das notwendige Maß iSv. Art. 5 Abs. 1 lit. c DSGVO gegeben, zumal der Notfall-Knopf zu jedem beliebigen Zeitpunkt gedrückt werden könne und somit eine dauerhafte Speicherung von Bilddaten auch ohne Unfallgeschehen möglich wäre.[19]

In einer anderen Entscheidung hielt die DSB fest, dass der Betrieb von Kameras, welche die vor einer *Wohnanlage* gelegenen, zur allgemeinen Nutzung bestimmten Flächen erfasste, gegen die in Art. 5 DSGVO normierten Grundsätze der Zweckbindung und Datenminimierung verstieß und verhängte eine Geldbuße in Höhe von EUR 1,000.[20]

Ebenso einen Verstoß gegen Art. 5 DSGVO stellte die DSB in einer Entscheidung fest, die Kameras eines Vereines betraf, welche im *Eingangsbereich* auf den öffentlichen Raum ausgerichtet waren. Dies insbesondere, da der Verantwortliche die Kameras durch eine Anpassung des Blickwinkels auf eine Weise betreiben hätte können, durch die ein Miterfassen der umliegenden öffentlichen Verkehrsflächen vermieden worden wäre.[21]

Pflichten des Verantwortlichen
Die DSB gab einer Beschwerde statt, die auf Löschung von Einträgen über ein nicht eröffnetes bzw. erledigtes Insolvenzverfahren in der Konsumenten- und Warenkreditevidenz gerichtet war. Die Beschwerdegegnerin hatte den Beschwerdeführer über diese Einträge nicht informiert; darüber hinaus war die Gläubigerforderung bereits zur Gänze beglichen worden. Die DSB hielt fest, dass aufgrund des in *Art. 5 Abs. 1 lit. a*

18 DSB 27.9.2018, DSB-D550.084/0002-DSB/2018 (rechtskräftig).
19 DSB 9.7.2018, DSB-D485.000/0001-DSB/2018-II, DSB-D485.000/0001-DSB/2018 (Empfehlung).
20 DSB 20.12.2018, DSB-D550.037/0003-DSB/2018 (rechtskräftig).
21 DSB 18.12.2018, DSB-D550.015/0003-DSB/2018 (rechtskräftig).

DSGVO verankerten Grundsatzes von *Treu und Glauben* eine entsprechende Benachrichtigung des Beschwerdeführers gemäß *Art. 14 DSGVO* erforderlich gewesen wäre.[22]

In einem Verfahren, in welchem die Beschwerdeführerin mit Blick auf potentielle Hacker-Angriffe und Datenlecks die Verletzung des Grundrechts auf Geheimhaltung durch eine „unterlassene Pseudonymisierung" ihrer Daten im ELAK (Elektronischer Akt) vorbrachte, hielt die DSB fest, dass aus der DSGVO kein Recht des Betroffenen auf spezifische Datensicherheitsmaßnahmen oder spezifische Maßnahmen zur Datenminimierung iSv. Art. 5 Abs. 1 lit. c DSGVO abzuleiten sei.[23]

In einer weiteren Entscheidung hielt die DSB schließlich fest, dass dem Betroffenen bei einem Löschbegehren freistehe, auch die Löschung bloß eines Teiles seiner Daten zu begehren. Die Vorgehensweise der Verantwortlichen, ungeachtet eines bloß partiellen Löschbegehrens sämtliche personenbezogenen Daten des Beschwerdeführers zu löschen, verletze den Grundsatz von *Treu und Glauben*.[24]

3.2 Bundesverwaltungsgericht

Das Bundesverwaltungsgericht befasste sich bislang nur am Rande mit den *Grundsätzen des Art. 5 DSGVO*: So führte das Bundesverwaltungsgericht aus, dass eine an den Beschwerdeführer gerichtete E-Mail, welche in Kopie ("CC") an weitere Personen weitergeleitet wurde, eine Verletzung des *Rechts auf Geheimhaltung* darstelle.[25] In einem weiteren Verfahren *verneinte* das Bundesverwaltungsgericht einen *Verstoß gegen den Zweckbindungsgrundsatz* durch die mitbeteiligte Partei, die ihren Verwaltungsdirektor mit der Führung von datenschutzrechtlichen Verfahren betraut und ihm daher Korrespondenzen und Verfahrensinhalte weitergeleitet hatte.[26]

22 DSB 30.11.2018, DSB-D122.954/0010-DSB/2018 (nicht rechtskräftig).
23 DSB 13.9.2018, DSB-D123.070/0005-DSB/2018 (rechtskräftig).
24 DSB 5.12.2018, DSB-D123.211/0004-DSB/2018 (nicht rechtskräftig).
25 BVwG 1.10.2018, W253 2140428-1; ebenso ohne vertieftere Befassung vgl. BVwG 27.9.2018, W214 2196873-1 und BVwG 10.12.2018, W211 2188383-1.
26 BVwG 10.9.2018, W258 2134678-1.

Frage 4

4.1 Einwilligung

4.1.1 DSB[27]

Sowohl zur Rechtsgrundlage der Einwilligung als auch des berechtigten Interesses sind in Österreich bereits eine Reihe von Entscheidungen ergangen. Nachstehend werden zunächst einige ausgewählte Entscheidungen der DSB wiedergegeben (gegliedert nach Verfahrensart):

Amtswegige Prüfverfahren – Anforderungen an Einwilligungen

In einem bereits auf Basis der DSGVO eingeleiteten Prüfverfahren befasste sich die DSB mit einer Einwilligungserklärung im Beitrittsformular zu einem Automobilclub und verneinte deren „Freiwilligkeit". Die DSB sah das Kriterium der *Verständlichkeit* nicht erfüllt. *Erstens*, da die vorformulierte Einwilligungserklärung den Betroffenen suggerierte, lediglich entscheiden zu können *durch welches Medium* sie *Marketing-Zusendungen* erhalten möchten (per Post, elektronisch oder per Telefon). *Zweitens*, da die Einwilligung direkt vor der Unterschrift für den Abschluss der Mitgliedschaft platziert war, sodass die Optionalität der Einwilligung missverstanden werden konnte. *Drittens*, da durch den im unmittelbaren textlichen Zusammenhang stehenden Hinweis auf die Widerrufsmöglichkeit der Eindruck vermittelt wurde, einer Datenverarbeitung zu Marketingzwecken zunächst zustimmen zu müssen und diese erst sodann mittels Widerrufs unterbinden zu können („opt-out").[28]

In einem weiteren Prüfverfahren erklärte die DSB eine in einem Formular einer Allergieklinik verlangte Einwilligung in mehrerlei Hinsicht für unzulässig. *Erstens*, da in den bereitgestellten Informationen nach Art. 13 DSGVO neben der Einwilligung auch andere Rechtsgrundlagen angeführt wurden und somit der Einwilligung nicht mit der erforderlichen Klarheit zu entnehmen war, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage darstellte. *Zweitens*, da die Einwilligung zur *Datenverarbeitung* an die Zustimmung zur *unverschlüsselten Übermittlung* von Daten gebunden war, die Erforderlichkeit einer derartigen Datensicherheitsmaßnahme nach Art. 32 DSGVO allerdings allein vom Verantwortlichen zu beurteilen ist. *Drittens,* da eine „unwiderrufliche" Einwilligung der DSGVO widerspricht. *Viertens* führte die DSB aus, dass bei einem Haftungsausschluss für die unkorrekte und unvollständige Übermittlung von Daten

27 Zum Kopplungsverbot und Anforderungen an die Freiwilligkeit hinsichtlich Setzung von Cookies beim Besuch einer Webpage (Online-Zeitung) siehe Frage 5 (DSB 30.11.2018, DSB-D122.931/0003-DSB/2018).

28 DSB 31.7.2018, DSB-D213.642/0002-DSB/2018 (rechtskräftig).

Aspekte der Datensicherheit nach Art. 32 DSGVO betroffen sind, von denen mittels Einwilligung nicht zum Nachteil von Betroffenen abgewichen werden kann.[29]

In einem weiteren Prüfverfahren, in welchem die DSB die Gültigkeit der Einwilligungen von *Arbeitnehmern* zu einem *GPS-Überwachungssystem* in Dienstfahrzeugen überprüfte, kam sie ebenfalls zum Ergebnis, dass diese mangels *Freiwilligkeit* unwirksam sei. Die DSB hielt fest, dass eine Einwilligung im arbeitsrechtlichen Kontext zwar möglich sei, jedoch einem klar erkennbaren Vorteil des Arbeitnehmers dienen müsse, was gegenständlich nicht der Fall sei. Sie schloss allerdings nicht aus, dass ein derartiges System auf eine andere Rechtsgrundlage (zB. Art. 6 Abs. 1 lit. f DSGVO) gestützt werden könnte.[30]

Sonstige Bescheide – Nichtvorliegen einer Einwilligung

Die DSB stellte in einer weiteren Entscheidung eine Verletzung des *Rechts auf Geheimhaltung* fest, da der Beschwerdegegner eine auf einer Webseite veröffentlichte Telefonnummer des Beschwerdeführers, die dazu diente, als „Beratungshotline" für bedürftige Personen erreichbar zu sein, für einen *Werbeanruf* verwendet hatte. Die DSB führt aus, dass die Veröffentlichung der Telefonnummer nicht als Einwilligung zu Werbeanrufen anzusehen sei.[31]

In einem weiteren Bescheid untersagte die DSB *mangels Einwilligung* des Beschwerdeführers die Datenverarbeitung durch einen *digitalen Türspion,* der feststellte, wer sich im Aufnahmebereich befindet (Bildaufnahme iSd. § 12 Abs. 1 DSG).[32]

4.1.2 Bundesverwaltungsgericht

Im einem Bauverfahren, in welchem Beamte im Wohnbereich des Beschwerdeführers *Fotos von privaten Wohnungsbereichen* aufnahmen und dies auf eine vermeintliche Einwilligung stützen, stellte das Bundesverwaltungsgericht klar, dass sich behördliche Datenverarbeitungen grundsätzlich auf geeignete gesetzliche Grundlagen stützen müssen (eine *behördliche Datenverarbeitung* auf der Grundlage einer *Einwilligung* könne nur im *Ausnahmefall* denkbar sein).[33]

In einem Verfahren über Zulässigkeit der Veröffentlichung eines Disziplinarerkenntnisses unter Anführung des Namens und der Adresse des Betroffenen in einem Mitteilungsblatt einer Körperschaft öffentlichen Rechts hielt das Bundesverwaltungsgericht fest, dass eine *Satzungsbestimmung*, wonach rechtskräftige Erkenntnisse in Disziplinarverfahren in einem Mitteilungsblatt zu veröffentlichen sind,

29 DSB 16.11.2018, DSB-D213.692/0001-DSB/2018 (rechtskräftig).
30 DSB 8.8.2018, DSB-D213.658/0002-DSB/2018 (nicht rechtskräftig).
31 DSB 31.10.2018, DSB-D123.076/0003-DSB/2018 (rechtskräftig).
32 DSB 5.10.2018, DSB-D123.204/0005-DSB/2018 (nicht rechtskräftig).
33 BVwG 11.7.2018, W214 2183935-1.

nicht als *Einwilligung* der betroffenen Person im Sinne des Art. 4 Z 11 DSGVO zu qualifizieren ist.[34]

4.1.3 OGH

Auch der Oberste Gerichtshof (OGH) setzte sich bereits mit der Freiwilligkeit einer Einwilligung auseinander. Gegenstand des Verfahrens war eine Verbandsklage wegen Klauseln in Allgemeinen Geschäftsbedingungen eines TV-Anbieters. Der OGH gelangte dabei zum Ergebnis, dass bei einer Kopplung der Einwilligung zur Verarbeitung vertrags*un*abhängiger personenbezogener Daten mit einem Vertragsabschluss davon auszugehen ist, dass die Erteilung der Einwilligung grundsätzlich nicht *freiwillig* erfolgt. Der OGH leitete aus dem Spannungsverhältnis des Verordnungstextes (Art. 4 Z 11 und Art. 7 Abs. 4 DSGVO) und EwGr. 43 strenge Anforderungen an die Beurteilung der Freiwilligkeit einer Einwilligung ab.[35]

4.2 Berechtigte Interessen[36]

4.2.1 DSB

In ihren bereits zitierten Straferkenntnissen zum Betrieb privater Videoüberwachungsanlagen nahm die DSB nicht nur einen Verstoß gegen die Grundsätze gem. Art. 5 DSGVO an, sondern hielt auch fest, dass auf Seiten der Verantwortlichen *kein berechtigtes Interesse* am Betrieb der jeweiligen Bildaufnahme gegeben sei.[37]

In einem anderen Verfahren (gegenständlich war die Frage der Zulässigkeit der Veröffentlichung von Kontaktdaten eines Mannschaftsführers auf der Website eines Sportverbandes) hielt die DSB fest, dass das Geheimhaltungsinteresse des Betroffenen das Interesse an der Verarbeitung überwiege.[38] Weitere Verfahren befassten sich mit dem (fehlenden) berechtigten Interesse des Arbeitgebers, aufgrund des Aufbewahrens eines Aktenvermerks über Verfehlungen eines früheren Arbeitnehmers, eine Wiedereinstellung zu verhindern[39] oder mit der Abwägung zwischen den berechtigten Interessen von

34 BVwG 27.9.2018, W214 2196873-1.

35 OGH 31.8.2018, 6 Ob 140/18h.

36 Zum berechtigten Interesse des Arbeitgebers mittels eines Aktenvermerks bestimmen zu können, mit wem ein Dienstverhältnis (nicht) eingegangen werden soll (DSB 15.11.2018, DSB-D122.944/0007-DSB/2018) und zur Abwägung zwischen den berechtigten Interessen von Portalbenutzern und den berechtigten Interessen des auf dem Portal bewerteten Arztes (DSB 15.1.2019, DSB-D123.527/0004-DSB/2018) siehe Frage 7.

37 Siehe Frage 3 (Bildverarbeitung) und Datenschutzbericht 2018 (März 2019) 50.

38 DSB 12.11.2018, DSB-D123.032/0003-DSB/2018.

39 DSB 15.11.2018, DSB-D122.944/0007-DSB/2018; siehe auch Frage 7.

Portalbenutzern (Patienten) gegenüber den berechtigten Interessen des auf dem Portal bewerteten Arztes[40].

4.2.2 Bundesverwaltungsgericht

Das Bundesverwaltungsgericht ging bislang nur vereinzelt substantiell auf Art. 6 UAbs. 1 lit. f DSGVO ein:

In einer schon erwähnten Entscheidung (3.2 – Verletzung des Rechts auf Geheimhaltung, da eine an den Beschwerdeführer gerichtete E-Mail in Kopie ["CC"] an weitere Personen weitergeleitet wurde), befasste sich das Bundesverwaltungsgericht mit dessen Anwendungsbereich. Die E-Mail-Korrespondenz zwischen dem Beschwerdeführer, einem als Personalvertreter dienstfreigestellten Beamten, und seiner Abteilungsleiterin fand zum Zwecke der "Weitergewährung von Kosten für Arbeitsmittel, also Gehaltsansprüchen des Beschwerdeführers" statt. Die DSB führt aus, dass die Bestimmungen betreffend die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen auf den vorliegenden Sachverhalt *nicht* anzuwenden sind, da dies gem. Art. 6 UAbs. 1 lit. f DSGVO für von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen ausgeschlossen ist und die Überprüfung der Geltendmachung von Ansprüchen eines Beamten durch dessen Dienstbehörde eine Erfüllung derer Aufgaben darstellt.

Aus demselben Grund verneinte das Bundesverwaltungsgericht in einer weiteren – ebenfalls schon erwähnten – Entscheidung (4.1.2 – Zulässigkeit der Veröffentlichung eines Disziplinarerkenntnisses durch eine Körperschaft öffentlichen Rechts in ihrem Mitteilungsblatt) die Anwendbarkeit von Art. 6 UAbs. 1 lit. f DSGVO.

Frage 5

Diese Fragestellungen wurden in Österreich in erster Linie in Zusammenhang mit Art. 7 DSGVO bzw. EwGr. 43 DSGVO diskutiert.

In der juristischen Literatur wurde dazu die Auffassung vertreten, dass das Kopplungsverbot[41] dem Konzept des „cash for consent" nicht entgegenstehe, da die Datenverarbeitung als *Gegenleistung* zur Vertragserfüllung *erforderlich* sei.[42] So möchten *Feiler/Forgó*[43] berücksichtigt wissen, dass bei „cash for consent" die datenschutzrechtliche Einwilligung und die Erbringung des Dienstes zwar nicht notwendigerweise in einem rechtlichen, aber jedenfalls in einem *wirtschaftlichen* Austauschverhältnis stehen; die

40 DSB 15.1.2019, DSB-D123.527/0004-DSB/2018; siehe auch Frage 7.
41 Kastelitz in Knyrim, DatKomm Art. 7 DSGVO Rz. 33.
42 Kastelitz in Knyrim, DatKomm Art. 7 DSGVO Rz. 34-38.
43 Feiler/Forgó, EU-DSGVO – EU-Datenschutz-Grundverordnung, Art. 7 Rz. 9-11.

Erteilung der Einwilligung schaffe erst die wirtschaftlichen Voraussetzungen für die unentgeltliche Zurverfügungstellung der Waren oder Dienstleistungen, sodass insofern die Einwilligung für die Vertragserfüllung (wirtschaftlich) *erforderlich* sei und daher eine wirksame Einwilligung vorliege.

Da allerdings auch valide Argumente[44] dafür bestehen, dass die Bereitstellung der Daten als Gegenleistung für die Vertragserfüllung *nicht* erforderlich ist, ist nicht gesichert, dass die DSB oder mit dieser Frage befasste Gerichte dieser Argumentation folgen würden.

Diskutiert wurde weiters, ob die Freiwilligkeit einer Einwilligung nicht beeinträchtigt ist, wenn der als Gegenleistung für die Einwilligung gewährte Vorteil nur *geringen* Wert hat. Allerdings ist zu vermuten, dass Behörden und Gerichte an die „Freiwilligkeit" der Einwilligung auch insoweit strenge Anforderungen[45] stellen werden.

Schließlich wurde diskutiert, ob unabhängig von der Frage, ob eine Verarbeitung für die Vertragserfüllung „*erforderlich*" ist, eine Einwilligung trotz *Kopplung* wirksam sein könne. Dies, da es auch darauf ankommt, ob ein „*Abhängigmachen*" (iSd Art. 7 Abs. 4 DSGVO) vorliege. In diesem Zusammenhang hat es die DSB in einer jüngeren und viel diskutierten Entscheidung[46] als zulässig angesehen, wenn der Betroffene die *Wahl* hat und einen angebotenen Vorteil alternativ durch eine (auch kostenpflichtige) Variante erhalten kann, die keine Einwilligung zur Verarbeitung von personenbezogenen Daten umfasst. Im Ausgangssachverhalt stellte eine Online-Zeitung die Betroffenen vor die Wahl, entweder ein kostenpflichtiges Abo um EUR 6,00 pro Monat zu erwerben *oder* kostenlos auf die Inhalte zuzugreifen, dafür aber eine Einwilligung zum Werbetracking mittels Cookies zu erteilen. Die Datenschutzbehörde gelangte zum Ergebnis, dass diese Einwilligung *freiwillig* erteilt werden könne, da bei Nichtabgabe der Einwilligung *bei weitem kein wesentlicher Nachteil* drohe (Online-Abo als keine unverhältnismäßig teurere Alternative; es kann auf ein alternatives Informationsangebot anderer Zeitungen zurückgegriffen werden bzw. erscheint die Zeitung auch in gedruckter Form).

Kritiker der Entscheidung wendeten ein, dass für das Vorliegen der Freiwilligkeit nicht relevant sein sollte, ob auch andere Medien genutzt werden können. Auch führe die Alternative der Zahlungspflicht nicht zu einer genuin freiwilligen Zustimmung und bestehe die Gefahr, dass Datenschutz zum Luxusgut werde, wenn dieses „Pay or Okay"-Konzept von Unternehmen flächendeckend angewandt werde; denn jedenfalls im Fall ihrer Kumulierung könnten derartige entgeltliche Alternativen für den Einzelnen Nachteile

44 ZB. die gebotene restriktive Auslegung des Begriffs der „Erforderlichkeit"; personenbezogene Daten als nicht handelbares Gut; Fehlen einer direkten und objektiven Verbindung zwischen Zweck der Verarbeitung und Zweck der Vertragserfüllung.

45 So wie der OGH anlässlich der Prüfung der Gültigkeit einer datenschutzrechtlichen Einwilligung in AGB. OGH 31.8.2018, 6Ob140/18h.

46 DSB 30.11.2018, DSB-D122.931/0003-DSB/2018.

entfalten.[47] Befürworter sahen die Entscheidung demgegenüber als Anerkennung des Umstandes, dass es Unternehmen wirtschaftlich unmöglich ist, einen Dienst oder Inhalte anzubieten, ohne dadurch Umsätze – sei es direkt durch Entgelt der Nutzer oder indirekt durch Werbeeinnahmen – erzielen zu können.[48]

Frage 6

Als Beispiele, in denen eine automatisierte Verarbeitung einschließlich Profiling gem. Art. 22 DSGVO erlaubt sein kann, nennt EwGr. 71 DSGVO die Überwachung und Verhinderung von Betrug und Steuerhinterziehung. In diesem Sinne wurde in Österreich diskutiert, ob der Erlassung eines Steuerbescheides ein behördliches Profiling vorausgehen darf. Da ein solches nicht gesetzlich vorgesehen ist, wurde dies im Ergebnis verneint.[49]

Nach EwGr. 71 DSGVO fällt auch die automatische Ablehnung eines Online-Kreditvertrags unter eine solche automatisierte Verarbeitung. Auch insoweit (und soweit ersichtlich auch nicht in sonstigen Bereichen) hat Österreich keine auf Art. 22 (2) (b) DSGVO gestützte gesetzliche Regelungen erlassen.[50]

Frage 7

Das Recht auf Löschung ist in Österreich (§ 1 Abs. 3 Z 2 DSG) auch verfassungsgesetzlich gewährleistet.

7.1 Suchmaschinen

Aus dem Transparenzbericht von *Google* geht hervor, dass seit 29.5.2014 rund 13.800 Ersuchen um Entfernung aus Suchergebnissen aus *Österreich* einlangten, die rund 56,000 URLs betrafen.[51] Im Schnitt wurden etwas weniger als die Hälfte der URLs aus den Suchergebnissen entfernt. Ca 86% der Antragsteller waren Privatpersonen. Hinsichtlich folgender drei Domains wurden die meisten URLs aus den Google-Suchergebnissen entfernt: www.facebook.com; groups.google.com; www.youtube.com.

Hinsichtlich anderer Suchmaschinenbetreiber (zB. Bing, Yahoo, Baidu und Yandex) sind zu Österreich keine Zahlen verfügbar.

---

47 Kastelitz/Tschohl, Die „derStandard.at"-E der Datenschutzbehörde kritisch betrachtet – DSGVO: Freiwilligkeit der Einwilligung bei Cookies? VbR 2019, 39; Feiler/Schrems, Cookies oder Zahlen: Für und Wider zum Datenschutz-Spruch, 10.12.2018, derStandard.at.

48 Feiler/Schmitt, Die entkoppelte Einwilligungserklärung – DSGVO: Freiwilligkeit der Einwilligung bei Cookies? VbR 2019, 38.

49 Ehrke-Rabel/Hödl, Steuerbescheid und behördliches Profiling, Dako 2017, 50.

50 Haidinger in Knyrim, DatKomm Art. 22 DSGVO Rz. 35.

51 transparencyreport.google.com/copyright/overview?hl=de-DE (Juli 2019).

7.2 Aufsichtsbehörde

Laut DSB-Datenschutzbericht 2018 war das Recht auf Löschung eines der Schwerpunktthemen in Beschwerdeverfahren.[52] Nachstehend wird ein Überblick über ausgewählte Entscheidungen gegeben:[53]

7.2.1 Entscheidungen in der Sache – Erfolgreiche Beschwerden:[54]

- In einem „Übergangsverfahren" befasste sich die DSB mit der Notwendigkeit der Speicherung personenbezogener Daten. Der Beschwerdegegner hatte dem Löschbegehren des Beschwerdeführers zwar entsprochen, im Zuge dessen allerdings Name, Geburtsdatum und Adresse des Beschwerdeführers gespeichert, was ua. mit einem Verweis auf „sicher amtsbekannte Gründe" nach Art. 17 Abs. 3 lit. e DSGVO begründet wurde. Die DSB hielt fest, dass dies nicht genüge, um die Erforderlichkeit der Verarbeitung gem. Art. 17 Abs. 3 DSGVO zu belegen.[55]
- In einem weiteren Fall entschied die DSB, dass die Speicherung der Daten des Beschwerdeführers im Hinblick auf eine eventuelle zukünftige Kontaktaufnahme gemäß Art. 17 Abs. 1 lit. a DSGVO dann nicht notwendig sei, wenn dieser die Löschung seiner gesamten Daten verlangt und daraus zu schließen sei, dass eine derartige Kommunikation nicht mehr erfolgen werde (zudem Verletzung des Grundsatzes der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO).[56]
- Hinsichtlich eines auf Löschung von Bonitätsdaten durch einen Wirtschaftsauskunftsdienst gerichteten Begehrens führte die DSB aus, eine generelle Löschung bonitätsrelevanter Daten sieben Jahre nach Tilgung der Schuld sei im Hinblick auf Art. 6 Abs. 1 lit. f DSGVO unverhältnismäßig. Die Datenschutzbehörde trug dem Wirtschaftsauskunftsdienst auf, Bonitätsdaten zu löschen, die eine Inkassoforderung betrafen, die bereits vor Eröffnung des Insolvenzverfahrens getilgt worden war. Die Löschung von Daten zu einer erst im Insolvenzverfahren getilgten Forderung war demgegenüber nicht geboten, da die gesetzliche Frist zur Löschung dieses Verfahrens aus der Insolvenzdatei noch nicht abgelaufen war.[57]

7.2.2 Entscheidungen in der Sache – nicht erfolgreiche Beschwerden:

- Für zutreffend erachtete die DSB hingegen die gegen ein Löschbegehren von Bewerberdaten vorgebrachte Argumentation eines Verantwortlichen, Daten von

52 Datenschutzbericht 2018, 18.
53 Vgl. auch Datenschutzbericht 2018, 18 ff.
54 Zu DSB 30.11.2018, DSB-D122.954/0010-DSB/2018 und DSB 5.12.2018 DSB-D123.211/0004-DSB/2018 (Treu und Glauben) siehe Frage 3.
55 DSB 28.5.2018, DSB-D216.580/0002-DSB/2018 (rechtskräftig).
56 DSB 28.5.2018, DSB-D216.580/0002-DSB/2018 (rechtskräftig).
57 DSB 7.12.2018, DSB-D123.193/0003-DSB/2018 (nicht rechtskräftig).

Bewerbern mindestens sechs Monate zu speichern, um einen eventuellen binnen dieser Frist geltend zu machenden Anspruch auf Entschädigung wegen Verletzung des *Gleichbehandlungsgesetzes* abwehren zu können. Folglich kann einem Löschungsbegehren gemäß Art. 17 Abs. 3 lit. e DSGVO die Notwendigkeit der Speicherung von Daten zur Abwehr konkret bezeichneter Rechtsansprüche erfolgreich entgegengehalten werden.[58] (Als gegensätzlich zu dieser Entscheidung kann die zuvor ergangene Entscheidung der DSB vom 28.5.2018, DSB-D216.471/0001-DSB/2018, angesehen werden: Die DSB stellte darin fest, dass die Beschwerdegegnerin, ein Telekommunikationsunternehmen, die Beschwerdeführerin dadurch in ihrem Recht auf Geheimhaltung verletzte, indem sie *Stammdaten, Verkehrsdaten und weitere personenbezogene Daten* nach Beendigung des Vertragsverhältnisses über den zulässigen Zeitraum hinaus verarbeitete. Nach der DSB normiert § 207 Abs. 2 Bundesabgabenordnung eine Verjährungsfrist und keine Verpflichtung zur Aufbewahrung von Daten, weshalb *Stammdaten* gem. § 132 Abs. 1 Bundesabgabenordnung zulässigerweise nur für eine Dauer von sieben Jahren aufbewahrt werden dürfen. Hinsichtlich der auf § 99 Abs. 2 Telekommunikationsgesetz gestützten Speicherung von Verkehrsdaten für einen Zeitraum von sechs Monaten nach Durchführung des Bezahlvorganges erklärte die DSB, dass die gesetzliche Frist des § 99 Abs. 2 Telekommunikationsgesetz von drei Monaten nicht mit der Berufung auf interne Prozesse/den Postlauf auf sechs Monate ausgedehnt werde. Andere personenbezogene Daten seien nach Beendigung der Vertragsverhältnisse entsprechend dem Grundsatz der Speicherbegrenzung ungeachtet der abstrakt bestehenden Möglichkeit von Schadenersatz- oder sonstigen Forderungen des Betroffenen zu löschen).

– Die DSB wies eine weitere Beschwerde ab, in welcher der Beschwerdeführer vorbrachte, dass sein ehemaliger Dienstgeber sich weigerte, Krankenstandstage und einen Aktenvermerk, dass einer Wiedereinstellung des Beschwerdeführers nicht zugestimmt werde, zu löschen. *Hinsichtlich der Krankenstandstage* hielt die DSB fest, dass sowohl § 132 BAO als auch § 42 Abs. 1 ASVG eine rechtliche Verpflichtung im Sinne des Art. 17 Abs. 3 lit. b DSGVO zur Aufbewahrung normieren und eine Löschung daher erst nach sieben Jahren erfolgen müsse. *Betreffend des Aktenvermerks* liege keine unrechtmäßige Verarbeitung nach Art. 17 Abs. 1 lit. d DSGVO vor, weil der Beschwerdegegner ein berechtigtes (Dokumentations-)Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO vorweisen könne, welches die Interessen des Beschwerdeführers überwiege (der Aktenvermerk werde zudem drei Jahren nach Beendigung des Dienstverhältnisses gelöscht).[59]

58 DSB 27.08.2018, DSB-D123.085/0003-DSB/2018 (rechtskräftig).
59 DSB 15.11.2018, DSB-D122.944/0007-DSB/2018 (rechtskräftig).

- In einem weiteren Fall hatte die DSB zu beurteilen, ob einem Löschbegehren auch dann entsprochen wurde, wenn die Daten des Beschwerdeführers nur teils durch vollständige Entfernung aus einem Kundenverwaltungs-System gelöscht wurden, teils aber durch bloße Entfernung des Personenbezugs („Anonymisierung"). Laut DSB komme dem Verantwortlichen hinsichtlich der Art und Weise, wie eine Löschung durchgeführt wird, ein Ermessen zu. Da die DSGVO auf Daten ohne Personenbezug keine Anwendung finde, könne die Entfernung des Personenbezugs („Anonymisierung") grundsätzlich ein zulässiges Mittel zur Löschung iSv. Art. 4 Z 2 iVm. Art. 17 Abs. 1 DSGVO darstellen. Es müsse aber sichergestellt sein, dass weder der Verantwortliche noch ein Dritter ohne unverhältnismäßigen Aufwand den Personenbezug wiederherstellen könne. Eine völlige Irreversibilität sei für das Vorliegen einer Anonymisierung iSd. DSGVO nicht notwendig.[60]
- Hinsichtlich einer Bewertungsplattform für Ärzte, welche einem Löschbegehren eines Allgemeinmediziners nicht entsprach, kam die DSB (im Einklang mit der deutschen Rechtsprechung) zum Ergebnis, dass Art. 17 Abs. 1 lit. d DSGVO nicht erfüllt sei, da die berechtigten Interessen der Portalbenutzer (Patienten) gegenüber den Interessen des Beschwerdeführers überwiegen (§ 1 Abs. 2 DSG). Insbesondere berücksichtigte die DSB, dass das in Art. 11 GRC bzw. Art. 10 EMRK verankerte Recht auf Freiheit der Meinungsäußerung auch die Abgabe und den Empfang von Bewertungen bzw. Erfahrungsberichten umfasst.[61]

7.3 Bundesverwaltungsgericht

Bislang wurde zu Art. 17 DSGVO nur eine Entscheidung des Bundesverwaltungsgerichts veröffentlicht, die eine Verfahrensfrage zum Gegenstand hatte. Es überprüfte, ob die DSB eine Beschwerde zu Recht zurückgewiesen hatte, weil sich diese auf das Recht auf Löschung gemäß Art. 17 DSGVO und hilfsweise auf das Recht auf Berichtigung gemäß Art. 16 DSGVO stützte. Die DSB ging davon aus, dass ein solcher Antrag nicht § 24 Abs. 2 DSG entsprochen habe, der zwingend die Bezeichnung des als verletzt erachteten Rechts verlangt. Dem folgte das Bundesverwaltungsgericht nicht und führte aus, dass mangels gegenteiliger Regelung auch in Datenschutzbeschwerdeverfahren Haupt- und Eventualanträge kumuliert werden können.[62]

60 DSB 5.12.2018, DSB-D123.270/0009-DSB/2018 (rechtskräftig).
61 DSB 15.1.2019, DSB-D123.527/0004-DSB/2018 (rechtskräftig).
62 Bundesverwaltungsgericht 22.11.2018, W258 2209560-1.

Frage 8

8.1 Gesetz und Interpretation

Gestützt auf die Öffnungsklausel des *Art. 85 Abs. 2 DSGVO* wurden in Österreich *§ 9 Abs. 1 und 2 DSG* erlassen: § 9 Abs. 1 DSG befasst sich dabei mit der Datenverarbeitung zu *journalistischen Zwecken*, § 9 Abs. 2 DSG mit der Datenverarbeitung zu *wissenschaftlichen, künstlerischen oder literarischen Zwecken.* In der Literatur wurde § 9 DSG teils stark kritisiert und als unionsrechtswidrig bezeichnet:

So wurde bemängelt, dass Verarbeitungen nur dann privilegiert seien, wenn sie zu journalistischen *Zwecken „des Medienunternehmens oder Mediendienstes*" erfolgen. Da zB. selbständige Blogger und Pressestellen Daten nicht zu Zwecken eines Medienunternehmens oder Mediendienstes verarbeiten, liege insoweit eine Einschränkung des Anwendungsbereichs auf *„klassische" Medien* vor. Zumal Art. 85 DSGVO eine solche Einschränkung nicht vorsehe, umfasse § 9 DSG daher Tätigkeiten, die nach der EuGH-Rsp als „*journalistisch*" einzustufen seien, nicht.[63]

Hinsichtlich des Umfangs der Privilegierung ist § 9 Abs. 1 DSG als *gänzliche und pauschale Ausnahmeregelung* von den Vorgaben der DSGVO und des DSG konzipiert, ohne den Erforderlichkeitsvorbehalt in Art. 85 Abs. 2 DSGVO aufzugreifen. Auch dies wurde in der Literatur als unionsrechtswidrig gesehen, da leg cit die Mitgliedstaaten wohl nicht dazu ermächtigen sollte, zB. Ausnahmen von der Anwendbarkeit der Regelungen der DSGVO zu Rechtsschutz, Schadenersatz und Sanktionen vorzusehen.[64]

Hingegen sieht § 9 Abs. 2 DSG nur eine Ausnahme von DSGVO und DSG vor, *„soweit dies erforderlich ist"*; die Regelung ist auch insoweit differenzierter, als sie *Gegenausnahmen* vorsieht und zB. die Anwendbarkeit des Art. 5 DSGVO (allgemeine Datenschutzgrundsätze) ausdrücklich anordnet. In diesem Zusammenhang wird allerdings als unionsrechtswidrig angesehen, dass § 9 Abs. 2 DSG die Abwägung an die Rechtsanwender delegiert, anstatt die gebotene Abwägung zwischen den Grundrechten auf Datenschutz und Meinungsäußerungs- bzw. Informationsfreiheit gesetzlich vorzunehmen und dann im erforderlichen Umfang Ausnahmen vorzusehen.[65]

63 Jahnel/Krempelmeier, Medien und Datenschutz in Österreich in Lachmayer/Lewinski, Datenschutz im Rechtsvergleich (2019), 179 (188); Krempelmeier, Sind die datenschutzrechtlichen Privilegien des § 9 DSG unionsrechtswidrig? jusIT 2018, 188; Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl (2018) DSG § 9 Rz. 1-12.

64 Jahnel/Krempelmeier (2019), 179 (190); Krempelmeier (2018), Rz. 1-12.

65 Jahnel/Krempelmeier (2019), 179 (192); Krempelmeier (2018), Rz. 1-12.

8.2 Anwendung

Zur erwähnten Bestimmung des § 9 DSG existiert bislang soweit ersichtlich nur eine DSB-Entscheidung.[66]

Im Ausgangssachverhalt behauptete der Beschwerdeführer eine Verletzung im Recht auf Löschung, weil die Beschwerdegegnerin, die ein Online-Forum betreibt, die Löschung seiner Userkommentare verweigert hatte.

Die DSB führte in ihrer Entscheidung aus, dass journalistische Tätigkeiten nicht nur Medienunternehmen vorbehalten sind (EuGH 16.12.2008, C-73/07 Rz. 62) und für die Anwendbarkeit des Privilegs nach § 9 Abs. 1 DSG daher allein der Verarbeitungszweck entscheidend sei. Daher könne § 9 Abs. 1 DSG ungeachtet seines restriktiveren Wortlauts auch „Bürgerjournalismus" (bspw. Internet-Diskussionsforen) umfassen, der den Zweck der einseitigen oder wechselseitigen Kommunikation von Ideen, Meinungen und Informationen verfolgt.

C Nationale Durchsetzung von Datenschutzrecht

Frage 9

9.1 Behörde und Zusammensetzung

Die DSB ist nationale Aufsichtsbehörde gemäß Art. 51 DSGVO (§ 18 DSG). Sie ist unabhängig (§ 19, 31 DSG).[67]

An ihrer Spitze steht ein Leiter, welcher wie sein Stellvertreter vom Bundespräsidenten auf Vorschlag der Bundesregierung für eine Dauer von fünf Jahren bestellt wird; die Wiederbestellung ist zulässig (§ 20 DSG). Als weiteres Personal waren der DSB im Jahr 2018 21 Juristen (davon zwei Praktikanten), 4 Mitarbeiter im gehobenen Dienst und 9 Mitarbeiter im Fachdienst zugeordnet.[68]

Durch die DSGVO wurde eine Umstrukturierung der DSB vorgenommen, indem diese in sechs Büros[69] unterteilt wurde (Präsidium; Verfahrensführung; Internationales und grenzüberschreitende Zusammenarbeit; Akkreditierung und Verhaltensregeln; Verwaltungsstrafen; sowie bis 27.12.2018 Stammzahlenregister).

66 Datenschutzbehörde 13.8.2018, DSB-D123.077/0003-DSB/2018.

67 Die genannten Bestimmungen wurden auch im Hinblick auf das zur früheren Organisation der DSB ergangene EuGH-Urteil vom 16.10.2012, C-614/10, *Europäische Kommission/Österreich*, erlassen, in welchem der EuGH festhielt, dass die zuvor bestehende Behördenorganisation dem Kriterium der Unabhängigkeit nicht ausreichend Rechnung trug.

68 Datenschutzbericht 2018 (März 2019) 9.

69 Ibid, 62.

9.2 Befugnisse oder Pflichten

Durch die DSGVO hat sich das Aufgabenspektrum der Datenschutzbehörde stark verbreitert[70] und sind insbesondere folgende Aufgaben hinzugekommen: Erlassung von Standardvertragsklauseln (Art. 28 Abs. 8 DSGVO); Entgegennahme und Prüfung von Meldungen über die Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO sowie Anordnung von Abhilfemaßnahmen; Erlassung von Verordnungen betreffend die (Nicht-)Durchführung einer Datenschutz-Folgenabschätzung unter Einbindung des Europäischen Datenschutzausschusses nach Art. 35 Abs. 4 und 5 DSGVO; Führung von Konsultationsverfahren nach Art. 36 DSGVO; Entgegennahme von Meldungen über die Bestellung von Datenschutzbeauftragten (Art. 37 Abs. 7 DSGVO); Prüfung und Genehmigung von Verhaltensregeln (Art. 40 DSGVO) sowie Erlassung der korrespondierenden Verordnung über die Akkreditierung von Überwachungsstellen (Art. 41 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses; Genehmigung von Zertifizierungskriterien (Art. 42 DSGVO) sowie Erlassung der korrespondierenden Verordnung über die Akkreditierung von Zertifizierungsstellen (Art. 43 DSGVO); Genehmigung von verbindlichen internen Vorschriften sowie von Vertragsklauseln zur Übermittlung von Daten an Empfänger in Drittstaaten oder internationalen Organisationen (Art. 46 f DSGVO); Führung von Verwaltungsstrafverfahren (Art. 83 DSGVO iVm. § 62 DSG); strukturierte Zusammenarbeit mit anderen Aufsichtsbehörden bei grenzüberschreitenden Fällen (Art. 60 f DSGVO); Mitarbeit im Europäischen Datenschutzausschuss (Art. 63 ff DSGVO).

Unverändert ist die DSB auch nach der neuen Rechtslage zuständig für Beschwerdeverfahren (Art. 77 DSGVO iVm. § 24 DSG); Amtswegige Prüfverfahren (Art. 57 Abs. 1 lit. h DSGVO); Verfahren betreffend Datenverarbeitung für Zwecke der wissenschaftlichen Forschung und Statistik (§ 7 DSG) sowie Datenverarbeitung von Adressdaten zur Benachrichtigung und Befragung von betroffenen Personen (§ 8 DSG).

Die DSB berät schließlich die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen (§ 21 DSB).

9.3 Rechtsdurchsetzungsbilanz

Obwohl die Anzahl der anhängig gemachten Verfahren im Vergleich zu 2017 signifikant angestiegen ist, konnten fast alle Verfahren innerhalb der gesetzlich vorgesehenen Frist von sechs Monaten beendet werden.[71] Im Jahr 2018 erledigte die DSB knapp 6,000 Eingangsstücke (darunter 509 Individualbeschwerden, 253 grenzüberschreitende Beschwerden (einlangend und ausgehend), 95 amtswegige Prüfverfahren, 119

70 Ibid, 7 ff.
71 Ibid, 64.

Genehmigungen im internationalen Datenverkehr, 344 Sicherheitsverletzungen und 3.974 Rechtsauskünfte).[72]

Frage 10

In den letzten Jahren hat die von der DSB zu bewältigende Fallzahl kontinuierlich zugenommen. Dies begründet durch den Zuwachs an Aufgaben und Befugnissen, andererseits aufgrund des iZm. der DSGVO gestiegenen Bewusstseins für Datenschutz. So stieg allein die Anzahl der eingelangten Individualbeschwerden von 180 im Jahr 2016 auf 1036 im Jahr 2018.[73] Von den 509 Erledigungen im Jahr 2018 wurde das Verfahren in 169 Angelegenheiten eingestellt und erging in 340 Fällen ein Bescheid.[74] Aus diesen Daten ist keine „*selective to be effective*"-Vorgehensweise ableitbar. Eine derartige „Strategie" stünde im Übrigen auch nicht im Einklang mit dem Verwaltungsverfahrensrecht, welches der DSB nicht erlaubt, eine Auswahl innerhalb der bei ihr anhängigen Verfahren zu treffen.

Die der DSB vom österreichischen Gesetzgeber in § 11 DSG nahegelegte Vorgehensweise („Ermahnen statt Strafen") wurde soweit ersichtlich bislang von der DSB negiert (diese hat in mehreren Fällen auch bei erstmaligen Verstößen Geldbußen verhängt – vgl. nachfolgend Frage 11).

Frage 11

Die Sanktionsmöglichkeiten wurden bislang von der DSB mit Augenmaß angewendet. Vor Inkrafttreten der DSGVO waren in Österreich die Bezirksverwaltungsbehörden für Verwaltungsstrafverfahren zuständig. Mit 25.5.2018 ging diese Zuständigkeit auf die DSB über. Die DSB übernahm alle bei den Bezirksverwaltungsbehörden anhängigen Verwaltungsstrafverfahren (in Summe 75) und leitete 2018 59 neue Verwaltungsstrafverfahren ein.[75] Ein Großteil dieser Fälle betraf Videoüberwachungen.[76] In den im Jahr 2018 (seit 25.5.2018) von der DSB geführten 134 Verwaltungsstrafverfahren erfolgten 83 Einstellungen, vier Ermahnungen und fünf Straferkenntnisse.[77] Die höchste 2018 verhängte Strafe belief sich auf EUR 4.800,-[78] und betraf die Videoüberwachung eines Geschäftslokals (Filmen des öffentlichen Raums, keine geeigneten Hinweisschilder, zu

72 Ibid, 10, 11.
73 Ibid, 10.
74 Ibid, 10.
75 Ibid, 49, 63.
76 Ibid, 49.
77 Ibid, 10.
78 Ibid, 50.

lange Speicherdauer, keine Protokollierung der Verarbeitungsvorgänge). Im Jahr 2019 verhängte die DSB im Vergleich schon merklich höhere Geldbußen: zB. EUR 10,000 gegen eine Privatperson wegen heimlichen Filmens anderer Personen; EUR 50,000 Euro gegen ein Unternehmen aus dem medizinischen Bereich wegen Verletzung der Informationspflichten und EUR 18 Mio gegen die österreichische Post, weil Daten zur Hochrechnung von politischen Affinitäten genutzt wurden.

Neben den Sanktionen der DSGVO bestehen noch folgende weitere Bestimmungen auf nationaler Ebene:

- Wie erwähnt wurde zunächst mit dem Datenschutz-Deregulierungsgesetz in § 11 DSG das Prinzip „Ermahnen statt Strafen" verankert („die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die *Verhältnismäßigkeit* gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch *Verwarnen* Gebrauch machen"). Begründet wurde die Einführung dieser Bestimmung damit, dass in Einklang mit Art. 58 DSGVO eine Beratung und eine Verwarnung möglich sein soll und eine Bestrafung nur unter Abwägung der Kriterien des Art. 83 DSGVO erfolgen soll.[79]
- In § 62 Abs. 1 DSG wurde (im Sinne des Art. 84 Abs. 1 DSGVO[80]) eine *Verwaltungsstrafbestimmung* geschaffen, welche subsidiär zur Anwendung kommt, sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist. So werden ua. widerrechtliche Zugriffe auf Datenanwendungen, Verletzungen des Datengeheimnisses, Verstöße gegen die im DSG geregelten Bestimmungen zur Bildverarbeitung und die Verweigerung der Einschau durch die DSB mit Geldstrafen bis zu EUR 50,000 sanktioniert.
- Schließlich sieht (wie bereits vor Inkrafttreten der DSGVO) § 63 DSG eine gerichtliche Strafbestimmung vor. Es handelt sich dabei um ein Vorsatzdelikt, das Datenverarbeitung in Gewinn- oder Schädigungsabsicht mit Strafdrohung von Freiheitsstrafen bis zu einem Jahr sanktioniert.

Frage 12

Die österreichische Rechtsordnung stand immateriellen Schadenersatzansprüchen lange skeptisch gegenüber. Grundsätzlich werden immaterielle Schäden nach österreichischer Rechtslage nur ersetzt, wenn deren Ersatzfähigkeit ausdrücklich gesetzlich angeordnet ist

79 21. Sitzung des Nationalrats, XXVI. GP, 20.4.2018, 31, zu Z 12 (§ 11), www.parlament.gv.at/PAKT/VHG/XXVI/NRSITZ/NRSITZ_00021/fname_721211.pdf.

80 Illibauer in Knyrim, DatKomm Art. 84 DSGVO Rz. 18 (Stand 1.10.2018, rdb.at).

(zB. Schmerzengeld bei Körperverletzung gem. § 1325 ABGB; Ersatz entgangener Urlaubsfreude gem. § 12 Abs. 2 PRG; ideelle Schäden bei Verletzung des Rechts am eigenen Bild gem. § 78 UrhG iVm. § 87 Abs. 2 UrhG; Ersatz ideeller Schäden gem. § 6 ff. MedienG). Die jüngere österreichische Rsp. zeigt sich dem allgemeinen Ersatz ideeller Schäden demgegenüber zugänglicher (vgl. Ersatz von Trauerschäden[81], Ersatz bei Vertauschung von Babys[82], ideeller Schaden bei vorsätzlichem Freiheitsentzug[83]), wenngleich die Höhe der zugesprochenen Beträge vergleichsweise gering ist.

Die Tendenz zu immateriellen Schadenersatzansprüchen ist auch im Datenschutz bemerkbar: In Österreich existierte bereits vor Inkrafttreten der DSGVO die Möglichkeit, immateriellen Schadenersatz für Datenschutzverletzungen geltend zu machen (§ 33 DSG 2000). Die diesbezüglichen Voraussetzungen waren allerdings restriktiv, weshalb derartige Ansprüche nur selten geltend gemacht wurden.[84]

Grundlage (DSG iVm. DSGVO)

Nach der nunmehr eingeführten Bestimmung des § 29 DSG hat jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück des DSG ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter nach Art. 82 DSGVO. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts und sind diese Ansprüche vor den ordentlichen Gerichten geltend zu machen.

Nach dem Wortlaut des § 29 DSG sind die Voraussetzungen im Vergleich zur früheren Rechtslage deutlich gelockert. Den Kläger trifft die Beweislast hinsichtlich des Eintritts eines (materiellen oder immateriellen) Schadens, hinsichtlich eines datenschutzrechtlichen Normverstoßes des Verantwortlichen und hinsichtlich der kausalen Verursachung des Schadens durch den Normverstoß des Verantwortlichen.

Bemessung

Die Bemessung der Höhe des immateriellen Schadenersatzes unterscheidet sich je nachdem um welchen Bereich es sich handelt: Schmerzengeld wird in „Tagessätzen" berechnet und es wird zwischen leichten, mittleren und schweren Schmerzen unterschieden.[85] Der Ersatz entgangener Urlaubsfreude wird in Pauschalbeträgen pro Tag abgegolten.[86] Hinsichtlich

81 *Reischauer* in *Rummel/Lukas*, ABGB[3] § 1325 Rz. 5a.
82 OGH 22.3.2018, 4 Ob 208/17t.
83 *Hinteregger* in *Kletečka/Schauer*, ABGB-ON[1.04] § 1329 Rz. 5.
84 Bsp OGH 6Ob275/05t 15.12.2005 (zur Aufnahme in die „Warnliste" der Banken); OGH 17.12.2009 6Ob247/08d (zur unzulässigen Eintragung in eine Bonitätsliste eines Kreditschutzverbands).
85 Welser/Zöchling-Jud, Bürgerliches Recht Band II[14] (2015) Rz. 1484.
86 ErläutRV 1513 BlgNR 25. GP 15.

des Ersatzanspruchs nach § 78 UrhG sollte die Höhe des immateriellen Schadenersatzes für den Verletzter fühlbar sein und der Allgemeinheit verdeutlichen, dass sich Rechtsverletzungen dieser Art nicht lohnen, wobei der Grad des Verschuldens sowie die Intensität und Dauer der Verletzung einfließen.[87] Im Zusammenhang mit § 6 MedienG muss die Zuerkennung von Schadenersatz für eine Ehrenkränkung nach der Rsp. des EGMR zu Art. 10 MRK in einem angemessenen Verhältnis zur erlittenen Beeinträchtigung des Ansehens stehen.[88]

Bei der Bemessung des immateriellen Schadenersatzanspruches für Datenschutzverletzungen nach § 33 DSG 2000 fielen bislang Faktoren wie die Intensität der Persönlichkeitsverletzung, der Verschuldensgrad des Schädigers, die Breitenwirkung der Datenveröffentlichung, Gewinnerzielungsabsichten des Schädigers und auch präventive Gedanken ins Gewicht. Da die Feststellung der Höhe eines immateriellen Schadens Schwierigkeiten bereiten wird, wird wohl häufig auf § 273 ZPO (Festsetzung durch freie richterliche Überzeugung) zurückgegriffen werden. Dabei werden Umstände des Einzelfalls ebenso bedeutend sein wie Beeinträchtigung des Opfers (Erfolgsunwert), Handlungsunwert, präventive Aspekte, Verbreitungsgrad sowie der Adressatenkreis der Datenschutzverletzung.[89]

Auf Basis der neuen Bestimmungen hat das LG Feldkirch im August 2019 (nicht rechtskräftig) einer Person wegen unrechtmäßiger Verarbeitung von besonderen Kategorien von Daten (hinsichtlich wahrscheinlicher politischer Affinitäten) EUR 800 an immateriellem Schadenersatz zugesprochen.[90]

Frage 13

13.1 Kollektiver Rechtsschutz

Österreich hat keine Regelungen getroffen, um kollektiven Rechtsschutz im datenschutzrechtlichen Kontext zu vereinfachen.

Dass die kollektive Rechtsdurchsetzung bei Datenschutzverstößen in der österreichischen Praxis Schwierigkeiten begegnet, zeigt sich nicht zuletzt an der öffentlichkeitswirksamen *Sammelklage gegen Facebook*, die 2014 von *Max Schrems* beim Landesgericht Wien wegen Verletzungen der Rechte auf Achtung der Privatsphäre und auf Datenschutz anhängig gemacht wurde.[91]

87 Guggenbichler in Kucsko/Handig, urheber.recht[2] § 87 UrhG Rz. 22-25.

88 Rami in Höpfel/Ratz, WK[2] MedienG § 6 Rz. 7.

89 Vgl. *Schweiger* in *Knyrim*, DatKomm Art. 82 DSGVO Rz. 30ff.

90 LG Feldkirch 07.08.2019, 57 Cg 30/19b.

91 Schrems vertrat dabei zunächst auch Verbraucher aus anderen EU-Staaten und Indien (vgl. ua OGH 28.2.2018, 6 Ob 23/18b; EuGH 25.1.2018, C-498/16, *Schrems*, ECLI:EU:C:2018:37 (infolge Vorlage des

13.2 Rolle von Nichtregierungsorganisationen

13.2.1 Art. 80 Abs. 1 DSGVO (Schadenersatz)

Die ursprünglich auch für Schadenersatzklagen vorgesehene Möglichkeit der Vertretung durch Nichtregierungsorganisationen wurde im Datenschutz-Deregulierungsgesetz 2018[92] wieder gestrichen. Betroffene haben daher auf Basis des § 28 DSG nur das Recht, eine Nichtregierungsorganisation zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und die in den §§ 24 bis 27 DSB genannten Schritte (Beschwerde an die Datenschutzbehörde, Begleitende Maßnahmen im Beschwerdeverfahren, Beschwerde an das Bundesverwaltungsgericht) zu setzen. Hingegen sind Nichtregierungsorganisationen nicht zur Geltendmachung von Schadenersatzansprüchen befugt, sondern gelten diesbezüglich die allgemeinen Bestimmungen der Zivilprozessordnung, welche eine Vertretung durch Rechtsanwälte vorsehen.

Kritisch gesehen wird dies naturgemäß von Datenschutzorganisationen wie noyb (noyb führt dazu aus, dass aufgrund der Möglichkeit, Ansprüche abzutreten, eine Schadenersatzklage gegen ein österreichisches Unternehmen einer „Vertretung" nach § 28 DSG nicht bedarf).[93]

13.2.2 Art. 80 Abs. 2 DSGVO (Verbandsklage)

In Österreich wurde zwar diskutiert, von der Öffnungsklausel in Art. 80 Abs. 2 DSGVO Gebrauch zu machen und so Nichtregierungsorganisationen unabhängig von einem Antrag der betroffenen Person die Befugnis einzuräumen, bei der Datenschutzbehörde Beschwerden eizureichen.[94] Letztlich wurde dies allerdings nicht umgesetzt.

13.2.3 Organisationen, Vereine, Anlaufstellen

Neben der schon angesprochenen Datenschutzorganisation „noyb" gibt es eine Reihe weiterer Anlaufstellen für Einzelpersonen, um Informationen zu erlangen bzw. Einrichtungen, die sich im Datenschutz engagieren; darunter:

– ARGE Daten, ein 1983 gegründeter österreichischer gemeinnütziger Verein, veröffentlicht auch Musterbriefe und allgemeine Informationen zum Datenschutzrecht.[95]

EuGH); zur letztendlichen Abweisung der Klage: futurezone.at/netzpolitik/facebook-klage-von-max-schrems-landesgericht-wien-nicht-zustaendig/400388459 (25.1.2019).

92 BGBl. I Nr. 24/2018; 21. Sitzung des Nationalrates der Republik Österreich, XXVI. Gesetzgebungsperiode, Freitag 20.4.2018, 31; AA-10 XXVI. GP – Abänderungsantrag.

93 Noyb, EU-Datenschutz: Regierungsparteien schwächen Rechtsdurchsetzung gegen globale Konzerne, noyb.eu/wp-content/uploads/2018/04/PA_DSGVO.pdf.

94 21. Sitzung des Nationalrates der Republik Österreich, XXVI. Gesetzgebungsperiode, Freitag 20.4.2018, 18.

95 www.argedaten.at/php/cms_monitor.php?q=AD-NEWS-LAST.

- Der Internet Ombudsmann, eine notifizierte Schlichtungsstelle iSd. § 4 Alternative-Streitbeilegung-Gesetz.[96]
- Der Verein für Konsumenteninformation (VKI), eine gemeinnützige Verbraucherschutzorganisation, veröffentlicht ebenfalls Musterformulare für Beschwerden bei der DSB sowie Musterauskunftsbegehren.[97]
- Die Arbeiterkammer tritt als Interessensvertretung für höhere Datenschutzstandards auf und veröffentlicht diverse Studien/Untersuchungen zu Datenschutzthemen (zB. Siri, Alexa, Cloud, Datenschutz von mobilen Apps).[98]
- Das Europäische Verbraucherzentrum Österreich unterstützt bei der außergerichtlichen Durchsetzung von Ansprüchen gegenüber einem Unternehmen im europäischen Ausland.[99]

Schließlich gibt es auf Datenschutz spezialisierte Forschungseinrichtungen wie zB. das Research Institute – Digital Human Rights Center (RI), welches ua. technische und rechtliche Aspekte des Datenschutzes und der Datensicherheit untersucht.[100]

Frage 14

14.1 Einschreiten anderer, bestehender Regulierungsbehörden

Es ist aktuell keine merkbare Tendenz in Österreich zu erkennen, dass neben der DSB auch andere Regulierungsbehörden auf Bundesebene in datenschutzrechtlichen Fragen einschreiten würden. Allerdings scheint durchaus möglich, dass datenschutzrechtliche Wertungen in die Beurteilung anderer österreichischer Regulierungsbehörden einfließen werden (wie etwa auch bereits das deutsche Bundeskartellamt).[101] Ebenso wie das Bundeskartellamt sind auch die österreichische Bundeswettbewerbsbehörde (BWB) und der österreichische Bundeskartellanwalt im Zuge der Kontrolle des Kartell- und Marktmissbrauchsverbots bzw. der Zusammenschlusskontrolle aufgrund der durch die Digitalisierung ermöglichten neuen Geschäftsmodelle/-methoden (etwa Preis-Algorithmen bzw. „Dynamic Pricing") immer häufiger mit Datenschutzfragen konfrontiert. Es ist daher denkbar, dass auch die BWB auf die DSGVO zurückgreifen würde, um Wettbewerbsverstöße zu begründen bzw. die Einhaltung von Auflagen im Datenschutzkontext anordnen könnte.

96 ombudsmann.at/schlichtung.php/cat/58/title/Datenschutz.
97 vki.at/musterbriefe.
98 www.arbeiterkammer.at/beratung/konsument/Datenschutz/index.html.
99 europakonsument.at/de/beschwerde-einbringen.
100 www.researchinstitute.at/christof-tschohl.html.
101 Beschluss des Bundeskartellamts vom 6.2.2019, B6-22/16.

14.2 Schaffung neuer Regulierungsbehörden für das Internet und für die künstliche Intelligenz

E-Government hat in Österreich einen hohen Stellenwert. Aktuell wird das „Digitale Amt" realisiert (Digitalisierung von Behördenwegen). Hingegen ist soweit ersichtlich nicht beabsichtigt, eine Internet- oder KI-Regulierungsbehörde zu schaffen.[102]

D Datenverarbeitung für nationale Sicherheitsbelange

Frage 15

Das DSG definiert den Begriff „nationale Sicherheit" nicht. In seinem 3. Hauptstück („*Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs*") nimmt das DSG allerdings auf den Begriff Bezug (in § 36 DSG im Zusammenhang mit dem Anwendungsbereich und in § 43 Abs. 4 Z. 2 DSG im Zusammenhang mit den Informationsrechten der betroffenen Person).

Zur Umsetzung eines „*Quick-Freeze-Modells*" wurden 2018 ua. Änderungen der Strafprozessordnung *(„StPO")* und des Telekommunikationsgesetzes („*TKG*") beschlossen. Bei Vorliegen eines Anfangsverdachts bestimmter gerichtlich strafbarer Handlungen sollen Telekommunikationsanbieter aufgrund staatsanwaltlicher Anordnung verpflichtet werden, Telekommunikationsdaten weiter zu speichern. So wurde den Fällen des § 99 Abs. 2 TKG, in denen von Betreibern eines öffentlichen Kommunikationsnetzes oder -dienstes Verkehrsdaten nicht zu löschen sind, ein weiterer Anwendungsfall hinzugefügt (§ 135 Abs. 2b StPO und § 138 Abs. 2 StPO). Der Zugriff auf diese Daten soll allerdings nur unter der Voraussetzung eines konkreten Tatverdachtes und einer gerichtlichen Bewilligung möglich sein. In den Erläuterungen zum Strafprozessrechtsänderungsgesetz 2018 (17 Blg XXVI. GP) wird durch mehrfache Bezugnahme auf das EuGH-Urteil *Tele 2 und Watson* (zB. hinsichtlich der Kategorien von zu speichernden Daten, des Anfangsverdachts, der gerichtlichen Bewilligung) deutlich, dass sich jedenfalls der österreichische Gesetzgeber der Anwendung der GRC auf die Vorratsdatenspeicherung aus nationalen Sicherheitsgründen in Folge des EuGH-Urteils bewusst ist und diese akzeptiert.

102 Vgl. auch „Broschüre – Die Zukunft der Künstlichen Intelligenz in Österreich gestalten", ein Entwurf für eine österreichischen KI-Strategie, www.bmdw.gv.at/DigitalisierungundEGovernment/Strategien/Seiten/K%C3%BCnstliche-Intelligenz.aspx.

Belgium

Anneleen Van de Meulebroucke, Dries Van Briel and Justine De Meersman[*]

A Setting the Scene

Question 1

New legislation

The most important legal instruments implementing the General Data Protection Regulation in Belgian (federal) legislation are (i) the Act of 3 December 2017 on the creation of the Data Protection Authority and (ii) the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.[1]

Contents of the Framework Act

The Framework Act is the most important piece of legislation when it comes to the implementation of the GDPR and the Law Enforcement Directive.[2] The Framework Act takes advantage of several of the flexibilities offered by the GDPR, such as:

- Article 8(1) GDPR on children's consent: article 7 Framework Act lowers the age for children to give valid consent for the processing of their personal data with regard to a direct offer of information society services to 13 years.
- Article 35(10) GDPR on data protection impact assessments: article 23 Framework Act obliges a controller to carry out its own data protection impact assessment (hereinafter "DPIA") prior to a processing activity based on a legal obligation or a task

* Attorneys-at-Law at Eubelius CV, Brussels (Belgium).

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (hereinafter "GDPR"); Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (hereinafter "Framework Act"); Act of 3 December 2017 on the creation of the Data Protection Authority (hereinafter "NSA Act").

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

carried out in the public interest or in the exercise of official authority, even if a DPIA was already carried out in the context of the adoption of the legal basis.
- Article 37(4) GDPR on the designation of a Data Protection Officer (hereinafter "DPO"): article 21 Framework Act stipulates that private bodies that process personal data on behalf of a federal authority or to which a federal authority transfers personal data are obliged to designate a DPO if such processing of personal data entails a high risk to the rights and freedoms of data subjects.
- Article 85 GDPR on freedom of expression and information: the Framework Act includes exemptions in this regard, which are further discussed in Question 8.
- Article 87 GDPR on the national identification number: the Act of 25 November 2018 has fundamentally changed existing legislation regarding the use of the national registry number.[3] In principle public authorities and public or private institutions need authorisation from the Minister of the Interior to access, receive and/or use the data of the national registry number. Exemptions apply for e.g. police forces, judges of courts and tribunals, etc.[4]
- Article 89 GDPR on processing for archiving purposes, scientific or historical research purposes or statistical purposes: title 4 of the Framework Act is entirely devoted to this matter and includes possibilities to deviate from data subjects' rights, provided that the exercise of these rights risks to render the processing for archiving in the public interest, for scientific or historical research or for statistical purposes impossible or provided that the exercise of these rights would seriously impair processing and hence derogations are necessary to achieve the objectives.[5]

The Framework Act contains a chapter allowing restrictions on the rights of data subjects in the application of article 23 GDPR.[6] Restrictions exist for the processing of personal data that are obtained from or communicated to authorities involved in intelligence and security services, police and judicial services.[7] In these cases, for obvious reasons of safety and secrecy, a controller is not allowed to inform the data subject of the processing of his personal data.[8] Data subjects have alternative means to ask the National Supervisory Authority (hereinafter "NSA") to perform verifications with the authorities involved.

3 Act of 25 November 2018 containing various provisions with regard to the National Registry and the population registers (hereinafter "Act of 25 November 2018"); Act of 8 August 1983 regulating a national registry of natural persons (hereinafter "Act of 8 August 1983").
4 Art. 8(3) Act of 8 August 1983.
5 Art. 186 Framework Act.
6 Arts 11-17 Framework Act.
7 Arts 11 ff. and 14 ff. Framework Act.
8 Exceptions apply when (i) the controller is obliged to provide the information in the context of legal proceedings or (ii) in case the authority from which the data were obtained allows the controller to provide information.

Oversight role of the NSA

The NSA issues opinions on draft legislation and in this way has an oversight role in legislation that implies data processing.[9] We further elaborate on the NSA and its functioning in Question 9.

Question 2

The right to private life is enshrined in article 22 of the Belgian Constitution.[10] During the legislative process, the legislator's intention was to bring the content of article 22 as closely as possible in line with article 8 European Convention of Human Rights (hereinafter "ECHR") in order to avoid substantive differences.[11] Under article 22 Constitution every individual has the right to private and family life, except in the cases and under the conditions provided for by law. Any interference with this right has to be provided for by an act in the formal sense of the word, which differs from article 8 ECHR that applies a qualitative legality principle.

Separate legislation has been adopted to protect the processing of personal data as part of the right to private life. The first legislative act in this regard was the Belgian Act of 8 December 1992 regarding the protection of private life towards the processing of personal data (which after a legislative change in 1998 also implemented Directive 95/46/EC).[12] This act was withdrawn and replaced by the Framework Act following the entry into force of the GDPR.

The Belgian Constitutional Court interprets the right to private life broadly and considers the right to protection of personal data and information to be part of the right to private life. It does not make a formal distinction between the right to private life and the right to data protection.[13]

The Constitutional Court examines article 22 Constitution in combination with article 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter "Charter")

9 Art. 23 NSA Act.

10 Coordinated Constitution of 17 February 1994 (hereinafter "Constitution").

11 Preparatory works Constitution, Parl. St. Senaat BZ 1991-92, no. 100-4/5; Preparatory works Constitution, Parl. St. Kamer 1992-93, no. 997/5, p. 2.

12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (hereinafter "Directive 95/46/EC").

13 CC 15 March 2018, No. 29/2018, Rec. B.11; CC 14 July 2016, No. 108/2016, Rec. B.9. The automatic identification of the right to data protection and the right to private life is however criticised in legal doctrine (P. De Hert & D. De Bot, 'Artikel 22 Grondwet en het onderscheid tussen privacyrecht en gegevensbescherming-srecht. Een formele wet is niet altijd nodig wanneer de overheid persoonsgegevens verwerkt, maar toch vaak', VDB-CDPK, No. 4, 2013, pp. 358-373; R. Van Crombrugge et al, 'Bescherming van persoonsgegevens: is er ruimte voor een horizontale toepassing van het legaliteitsbeginsel in artikel 22 Gw.?', RW, No. 7, 2015, pp. 243-252.

and considers these rights in relation to the right to data protection to have a scope that is analogous to article 8 ECHR, article 22 Constitution and article 17 International Covenant on Civil and Political Rights.[14]

Regarding the right to data protection, the Constitutional Court assumes that the international obligations arising from Directive 95/46/EC are an integral part of the guarantees laid down in article 22 Constitution. Recently, the Constitutional Court has reconfirmed this reasoning by stating that Directive 95/46/EC and the GDPR must be taken into account in the assessment of the validity of legislation in light of article 7 and 8 Charter.[15]

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Principle of fair processing

The principle of fair processing is one of the three principles of lawfulness, fairness and transparency mentioned in article 5(1)(a) GDPR.

The NSA tends to interpret the principle of fair processing mostly in the light of transparency (articles 12 – 14 GDPR). The NSA especially underlines that controllers have the responsibility to ensure that data subjects are informed of (i) the purposes of processing, (ii) the identity of the controller with whom they can exercise their data subject rights and (iii) the risks of the processing as well as the data subject's rights (in line with recital 39 GDPR).[16]

The principle of fair processing was applied in the Facebook-case initiated by the former NSA. The NSA accused Facebook of tracking browsing behaviour of internet users, with and without a Facebook account, by using social plug-ins, cookies and pixels without user consent. The Brussels Court of First Instance ruled that fair processing requires data to be obtained transparently and to be kept no longer than necessary and that subsequent processing does not conflict with reasonable expectations of data subjects. A lack of sufficient information by Facebook about systematic tracking on third party websites not

14 CC 19 July 2018, No. 96/2018; CC 15 March 2018, No. 29/2018, Rec. B.15.1; CC 14 July 2016, No. 108/2016, Rec. B.13.1; CC 6 December 2012, No. 145/2012; CC 14 December 2005, No. 189/2005.

15 CC 15 March 2018, No. 29/2018, Rec. B.15.2.

16 See for recent examples: NSA, Opinion No. 135/2018 of 28 November 2018, No. 47 and NSA, Opinion No. 132/2019 of 3 July 2019, No. 32; NSA, 'Principe de traitement licite, loyal et transparent', www.autoriteprotectiondonnees.be/principe-de-traitement-licite-loyal-et-transparent. All webpages referred to were visited 11 February 2020.

only led to a lack of valid consent (see Question 4), but also entailed a violation of the principle of fair processing.[17]

In a recent decision, the NSA determined that a controller must take appropriate measures to ensure that data subjects receive the information required by article 13 GDPR in a concise, transparent, comprehensible and easily accessible form and in 'clear and simple language'.[18] Policies must contain accurate and complete information and the controller must provide appropriate means (e.g. a link to the privacy policy) to make the policies easily available to data subjects in all languages of the website.

Principle of data minimisation

The NSA interprets the principle of data minimisation in the same fashion as article 5(1)(c) GDPR and recital 59 GDPR. On its website, the NSA recommends data controllers to only process the strict minimum of data required. A review of whether all data is adequate, relevant and limited to what is necessary with regard to the purposes is part of the standard check of the NSA when assessing draft legislation.[19]

So far, there have been two decisions from the NSA relating to data minimisation.

In a first decision, the NSA decided that the mere fact of placing a surveillance camera in a kitchen of a student dorm is a violation of the data minimisation principle because the kitchen is a common space where residents have no other choice than to enter and being filmed.[20]

In a second decision, the NSA decided a case where a company required a scan of the customer's eID in exchange for a loyalty card.[21] By scanning the eID the company automatically received the customer's national registry number. As explained above (see Question 1), use of this number is subject to strict rules. The NSA considered the use of the number as a means to retrieve customer data in the company's database disproportionate. Furthermore, the NSA considered the processing of gender and birth date disproportionate because the loyalty card was not used for verifying the minimum age of the customer. The company was imposed a fine of 10,000 euro (also because of other infringements – see Question 4).

17 Court of first instance Brussels 16 February 2018, RABG, No. 9, 2019, p. 695. Facebook appealed against this judgment. The Brussels Court of Appeal decided on 8 May 2019 to refer certain preliminary questions to the EU Court of Justice. An excerpt of the decision of the Court of Appeal Brussels can be found here: www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Dispositief_arrest.pdf; Request for a preliminary ruling from the Court of Appeal Brussels of 8 May 2019, C-645/19 Facebook Ireland and Others. The questions relate to the international jurisdiction of the court.

18 NSA, Decision No. 11/2019 on the merits of 25 November 2019.

19 NSA, 'Principe de minimisation des données', www.autoriteprotectiondonnees.be/principe-de-minimisation-des-donn%C3%A9es. See for a recent example: NSA, Opinion No. 132/2019 of 3 July 2019, Rec. 24.

20 NSA, Decision No. 03/2019 on the merits of 2 April 2019.

21 NSA, Decision No. 06/2019 on the merits of 17 September 2019.

Principle of purpose limitation

Finally, the NSA interprets the purpose limitation principle in the same way as and with reference to the European sources (article 5(1)(b) GDPR and 6(4) GDPR).[22] The (Litigation Chamber of the) NSA had the opportunity to apply the principle of purpose limitation in five recent decisions.

In a first decision, the NSA decided that the coordinator of a neighbourhood watch who (re)used personal data obtained through a WhatsApp Group of the neighbourhood watch to send emails with personal election propaganda infringed the purpose limitation principle. The coordinator admitted his one-off mistake and got away with a reprimand.[23]

In a second decision, the NSA decided that a company that had sent a global email to all its customers in order to sign a tax declaration, whereby all customers were visible instead of using the bcc-field, infringed the purpose limitation principle. Interestingly, the NSA also found an infringement of the principles of accountability and privacy by design and by default (article 24-25 GDPR). The company did not contest the facts and received a reprimand.[24]

In a third decision, the NSA decided that a mayor who (re)used email addresses of citizens obtained during his office (i.e. a decision on allotment) for sending personal election propaganda infringed the purpose limitation principle. The mayor received an administrative fine of 2,000 euro.[25]

In two other similar cases, the NSA imposed an administrative fine of 5,000 euro each on a mayor and an alderman for misusing personal data for electoral purposes.[26] The mayor used personal data that he had obtained in his capacity as mayor. The alderman used a client list that he had obtained in the context of his professional activities.

Question 4

In recent guidelines, the NSA paid specific attention to the legal bases for the processing of personal data in the context of direct marketing.[27] The NSA clarified that there is no hierarchy between the legal grounds provided by the GDPR and that a controller must

22 NSA, 'Principe de finalité déterminée', www.autoriteprotectiondonnees.be/principe-de-finalit%C3%A9-d%C3%A9termin%C3%A9e.

23 NSA, Decision No. 01/2019 on the merits of 2 April 2019.

24 NSA, Decision No. 02/2019 on the merits of 2 April 2019.

25 NSA, Decision No. 04/2019 on the merits of 28 May 2019.

26 NSA, Decision No. 10/2019 on the merits of 25 November 2019; NSA, Decision No. 11/2019 on the merits of 25 November 2019.

27 NSA, Recommendation no. 01/2020 of 17 January 2020, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Recommandation_01-2020_marketing_direct.pdf.

demonstrate that the processing is validly based on the legal grounds laid down in article 6 GDPR (and article 9(2) GDPR, if applicable).[28]

Regarding the legal ground of legitimate interests, the interest of the controller to process personal data should, according to the NSA, always prevail over the interest of the data subject not to process the data.[29] The NSA specifies that the NSA or a judge should decide whose interest prevails in a given case. In the case regarding the use of the eID to obtain a loyalty card (see Question 3), the NSA assessed the interests of both the company and the data subject and found the interests of the data subjects to prevail. Therefore, the company could not rely on the legal ground of legitimate interests.

In a recent case on the use of cookies, the NSA elaborated on consent as a legal basis for placing cookies. The NSA first of all decided that consent is required for all types of non-essential cookies. Furthermore, the NSA ruled that consent is only valid if the user has received accurate and adequate information about the cookies in advance. Finally, the NSA clarified that the user should be able to choose between all types of (non-essential) cookies and should actively consent for each type of cookies separately. Pre-ticked boxes are not allowed.[30]

One of the most notorious cases on consent brought before a national court was, again, the Facebook-case (see Question 3), where the Brussels Court of First Instance ordered Facebook to stop tracking internet traffic of Belgian internet users via cookies and other technologies without their consent.[31] A cookie banner warning internet users that Facebook places cookies on the basis of further browsing was not considered sufficient in this regard. Facebook's defence that it could also rely on a legitimate interest, was rejected.[32]

Question 5

The EU recently adopted Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.[33] The Directive Digital Content & Digital Services contains a framework for the payment of digital content and digital services with (personal) data.

28 NSA, Recommendation no. 01/2020 of 17 January 2020, p. 46.

29 NSA, 'Intérêt légitime', www.autoriteprotectiondonnees.be/lexique/interet-legitime.

30 NSA, Decision No. 11/2019 on the merits of 25 November 2019.

31 Court of First Instance Brussels 16 February 2018, RABG, No. 9, 2019, p. 695.

32 Facebook referred to its interest in security in relation to the use of the datr-cookie and its interest in advertising based on surf behaviour and optimisation in relation to the fr-cookie (Facebook pixel).

33 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 (hereinafter "Directive Digital Content & Digital Services").

In the context of the draft proposal of the directive, the Belgian Council for Consumption issued an opinion in 2016 and commented on the issue of data as a counter performance for a service.[34] In this opinion, representatives of businesses did not support the application of the same set of rules to both agreements for the supply of digital content in exchange for the payment of a price and agreements in exchange for data as a counter performance. These representatives hence favoured a more restricted scope of the directive, limited to the sale of digital content in exchange for a price. They argued that a broad material scope would hamper innovation as it entails a lot of formalities for businesses. Representatives of consumers, on the contrary, welcomed the proposal and suggested enlarging the scope of the directive even more in order to also include agreements in exchange for passively provided data.

Question 6

In 2019, the NSA advised on three occasions on draft legislative acts that introduce profiling measures.[35] The most interesting advice of the NSA relates to a draft act entrusting an energy regulator with the power to grant authorisations for collective self-consumption of energy based on a study of the energy consumption profile of the applicant.[36] In this case, the NSA advised the legislator to include the following safeguards in the legal basis: (i) a description of the role of the regulator who carries out the processing (controller/processor), (ii) legal remedies against the decision of the regulator, (iii) the right for the data subject to express his or her point of view (e.g. in case the regulator refuses an authorisation based on exceptional consumption figures) and (iv) the methodology of the profiling.

More recently, the control organ for police information ordered the immediate termination of a pilot project with facial recognition at the national airport because of a lack of legal ground, the lack of carrying out a DPIA and problems with false positives and negatives.[37]

34 Proposal for a European directive on certain aspects of contracts for the supply of digital content of 5 July 2016. The Council for Consumption is an advisory body for the department of economy ("Raad voor het Verbruik"): Raad voor het Verbruik, 'Advies betreffende het voorstel van Europese Richtlijn betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud', RvV 494, Brussels, 5 July 2016, www.economie.fgov.be/sites/default/files/Files/About-SPF/avis-cc-rvv/Advies-494-Raad-Verbruik.pdf.

35 NSA, Opinion No. 116/2019 of 5 June 2019; NSA, Opinion Nos. 44/2019 and 32/2019 of 6 February 2019.

36 NSA, Opinion No. 44/2019 of 6 February 2019.

37 P. Heymans & A. Vanrenterghem, 'Politie mag geen automatische gezichtsherkenning meer gebruiken op de luchthaven', www.vrt.be/vrtnws/nl/2019/09/20/politie-mag-geen-automatische-gezichtsherkenning-gebruiken-op-de/.

Question 7

In one of its first decisions, the NSA ordered a company to delete the data of a data subject after three previous requests had been ignored.[38]

Under the reign of the former NSA, a case was brought by a person accused on different websites of being involved in child abduction and paedophilia although he had never been the subject of criminal investigations.[39] The former NSA advised the search engine to implement deletions of search results on all domains, except to the extent that it was demonstrated for a given country that the right to be forgotten would infringe upon national law.[40] The former NSA furthermore urged the search engine to enhance the effectiveness of its deletion mechanisms (e.g. deletion of "first name + name" is not enough).

The right to erasure (right to be forgotten) was also the subject of two landmark decisions of the Court of Cassation.

The first case related to the publication of an online news archive by a newspaper in 2008. This archive contained reproductions of older articles, among which a feature on a traffic accident in 1994 caused by the claimant which mentioned the claimant by his name. Because the newspaper ignored the claimant's request to remove the article or at least to anonymize it, he started legal proceedings invoking *inter alia* his right to be forgotten. The Court of Cassation considered that the rights to freedom of expression and press freedom include the right for publishers to put digital archives online, but that these rights must be balanced against a person's right to private life and right to be forgotten. The Court concluded that the online archive is a new disclosure of the claimant's criminal history that interferes with, and in the case at hand violates, his right to be forgotten. As such, the Court confirmed the lower court's decision to award a compensation for moral damage (1 euro) and to anonymise the article.[41] A similar judgment was issued by the Court of Cassation on 8 November 2018.[42]

38 NSA, Decision No. 02/2019 of 15 May 2019. In two other decisions of the NSA on complaints from data subjects for non-compliance with their right to erasure, the NSA decided to dismiss the case (NSA, Decision No. 09/2019 on the merits of 17 September 2019) or it found that there was no infringement (NSA, Decision No. 08/2019 on the merits of 17 September 2019).

39 Former NSA, advice 75/2017 of 13 December 2017 following a complaint against a search engine regarding the modalities of the implementation and the geographic extent of deleting URLs from search results.

40 Compare with Judgment of 24 September 2019 in Case C-507/17, Google LLC, venant aux droits de Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772; Judgment of 3 October 2019 in Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited, ECLI:EU:C:2019:821.

41 Cass. 29 April 2016, C.15.0052.F.

42 Cass. 8 November 2018, C.16.0457.F.

Question 8

The Framework Act contains a chapter on the processing for journalistic purposes and for academic, artistic or literary expression.[43] Processing for journalistic purposes is defined as the preparation, collection, drafting, production, distribution or archiving for the purpose of informing the public, regardless of the medium, whereby a controller is responsible for compliance with journalistic deontological rules.[44] The Framework Act does not contain definitions of processing activities for academic, artistic or literary forms of expression.

Processing activities for journalistic purposes and for academic, artistic or literary expression can benefit from four kinds of alleviations under Belgian law:

- The rules regarding consent and processing of special categories of data (article 7 – 10 GDPR) and certain rights of data subjects, e.g. the right to rectification, to restriction of processing and to data portability (article 11(2), 16, 18, 19, 20 and 21(1) GDPR) are not applicable.
- There are fewer obligations to cooperate with supervisory authorities (e.g. records of processing activities do not need to be made available to supervisory authorities, data breaches do not need to be notified) if these obligations would compromise a publication or would constitute a control measure prior to a publication (articles 30(4), 31, 33 and 36 GDPR).
- The rules on data transfers (articles 44 – 50 GDPR) do not apply if that is necessary to reconcile the right to data protection with the right to freedom of speech and of information.
- The powers of supervisory authorities (article 58 GDPR) cannot be used if they can unveil sources or would constitute a control measure prior to a publication.

To our knowledge, these new articles have not yet been at stake before the Belgian courts or the NSA.

The CJEU, in its judgement of 14 February 2019, interpreted the journalistic exception broadly, by ruling that a video post on YouTube by a non-professional journalist constitutes the processing of personal data for journalistic purposes provided that the purpose of the recording and publication is solely to make information, opinions or ideas known to the public.[45] In the light of that judgment, the Belgian legislator might have to reconsider the scope of article 24(1) Framework Act, which limits the journalistic exception from the

43 Title I, Chapter V Framework Act.

44 Art. 24 Framework Act. It remains to be seen how this definition can be upheld in the light of the CJEU's Judgment of 14 February 2019 in Case C-345/17, *Sergejs Buivids v. Datu valsts inspekcija*, ECLI:EU:C:2019:122.

45 Case C-345/17, *Buivids*, para. 69.

obligations under GDPR to "*the controller responsible for compliance with journalistic deontological rules*".

C Domestic Enforcement of Data Protection Law

Question 9

The main supervisory authority in Belgium is the Data Protection Authority (see Question 1). There are different sector-specific supervisory authorities for processing activities by the police, the intelligence and security services.[46]

The NSA is composed of six bodies:

i. the Executive Committee ("Comité de direction");
ii. the General Secretariat ("Secrétariat général");
iii. the Front Office ("Service de première ligne");
iv. the Knowledge Centre ("Centre de connaissance");
v. the Inspection Service ("Service d'inspection"); and
vi. the Litigation Chamber ("Chambre contentieuse").[47]

The members of the Executive Committee, the Knowledge Centre and the Litigation Chamber are appointed by the Belgian Federal House of Representatives for a one-time renewable term of six years.[48]

In addition, the NSA is supported by an independent Reflection Council ("Conseil de réflexion"). The Belgian Federal House of Representatives decides on the composition of the Reflection Council and appoints its members. The members of the Reflection Council are, however, not part of the NSA.[49]

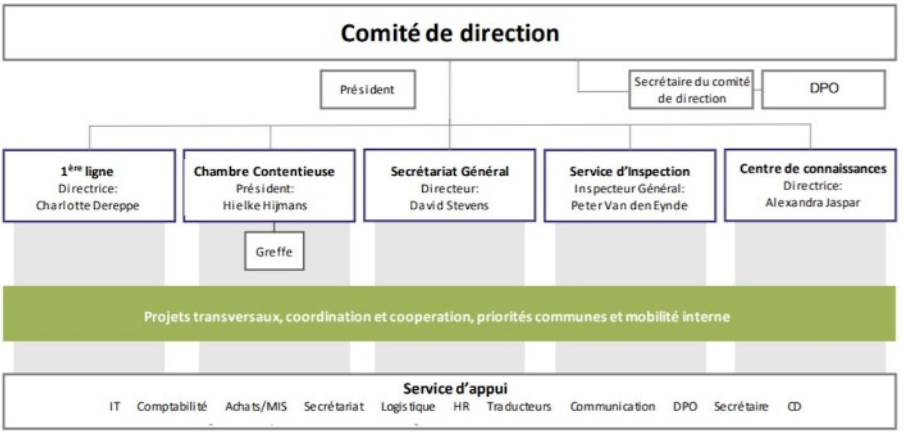
46 Arts 95, 128 and 161 and 184 Framework Act determine the power of the Control Organ of Police Information, the Standing Intelligence Agencies Review Committee and the Standing Police Monitoring Committee. At regional level, the Flemish supervisory commission ("Commission de contrôle flamande pour le traitement des données à caractère personnel") is specifically competent for the data processing by the Flemish public authorities. The counterparts of the Flemish supervisory commission at Brussels and Walloon level are currently not yet fully-fledged supervisory authorities within the meaning of the GDPR.

47 Art. 7 NSA Act.

48 Art. 37 read together with art. 39 NSA Act.

49 Art. 35 NSA Act.

Figure 1 organisational model NSA (NSA, Strategic plan 2019-2025, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_2019-2025.pdf, p. 33)



The NSA has the powers and duties as foreseen by the GDPR. Although not specifically provided for in the GDPR, the Front Office is specifically competent to initiate a mediation procedure.[50]

In 2018, the NSA initiated 218 audit files and several administrative sanctions have been imposed meanwhile.[51]

On 12 December 2019, the Executive Committee released its strategic plan with the annual priorities of the NSA. In the coming years, the NSA will mainly focus on five key sectors: (1) telecommunications and media, (2) government, (3) direct marketing, (4) education and (5) small and medium-sized enterprises ("SMEs"). In addition, the NSA will also pay specific attention to the role of data protection officers, the legitimacy of the processing activity and data subject rights. Finally, the NSA will respond proactively to three particular issues that it considers to be high on the societal agenda: 1) the creation and use of photos and cameras, 2) online privacy and 3) use of sensitive data (including biometric data).[52]

50 Art. 22(2) NSA Act.

51 NSA, 'Rapport Annuel 2018', www.gegevensbeschermingsautoriteit.be/jaarverslag-rapport-annuel/fr/politique-de-respect-des-dispositions-legales-information-et-assistance-dans-l-exercice-des-droits-et-des-obligations.html.

52 NSA, 'Plan Stratégique 2019-2025', www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_2019-2025.pdf, pp. 22-27.

Question 10

Any person can submit a complaint to the NSA.[53] The NSA has established a template form on its website.[54] Filing a complaint is in principle free of charge.

The legislator has taken into account the NSA's concern to be able to act selectively in view of an effective and efficient enforcement policy at every stage of the complaint procedure.[55]

- The Front Office first examines whether the complaint is admissible.[56] The Front Office has a margin of discretion considering the priorities set by the Executive Committee and the seriousness of the complaint.[57] The Front Office may also initiate a mediation procedure between the parties.[58]
- The Front Office submits admissible complaints to the Litigation Chamber.[59] The Litigation Chamber can deal with the complaint in two ways: either it chooses a 'light procedure' (i.e. without hearing the parties or presenting their defense) or it chooses to deal with the merits of the case.[60] The Litigation Chamber also has the power to dismiss the case.[61]
- The Litigation Chamber can (but is not obliged to) ask the Inspection Service to carry out an investigation before taking a decision.[62] The Inspection Service then submits an investigation report to the Litigation Chamber.[63]

An investigation by the NSA can also be triggered in other ways, i.e. without receiving a complaint. For instance, the Inspection Service may start investigations at its own initiative or at the request of the Executive Committee.[64]

53 Art. 58 NSA Act.
54 NSA, 'Procédures', www.autoriteprotectiondonnees.be/introduire-une-requete-une-plainte.
55 Preparatory works NSA Act, Parl. St. Kamer 2016-17, no. 54 2648/001 (hereinafter "Preparatory works NSA Act"), p. 51.
56 Art. 60 NSA Act.
57 Preparatory works NSA Act, p. 41.
58 Art. 22(1)(2) NSA Act.
59 Art. 62(1) NSA Act.
60 Preparatory works NSA Act, pp. 51-52. This procedure is criticised in legal doctrine: see L. Kuyken et al, 'Handleiding bij inspectie door de GBA', TPP, No. 1, 2019, p. 11.
61 Art. 95(1)(3) and art. 100(1) NSA Act; see for example NSA, Decision 09/2019 on the merits of 17 December 2019 and NSA, Decision 05/2019 of 23 July 2019.
62 Art. 94(2) NSA Act; Kuyken e.a., 2019, p. 7.
63 Art. 91(1) NSA Act; Preparatory works of the NSA Act, p. 49.
64 Art. 63(1) NSA Act.

In its strategic plan, the NSA underlines that it does not intend to act only on the basis of complaints. By contrast, it intends to strive for an open and innovative organisation with proactivity as one of its core values.[65]

Question 11

The Litigation Chamber is the NSA's administrative dispute body and has the power to take all corrective measures and impose administrative fines as set out in articles 58(2) and 83 GDPR. In addition, the Litigation Chamber has the power to impose periodic penalty payments ("astreintes") and it can decide to publish decisions on its website (which happens frequently).[66]

Based on the published decisions of the Litigation Chamber, the Litigation Chamber has so far imposed different sanctions:

- a warning (e.g. NSA, Decision 04/2019 of 28 May 2019);
- a reprimand (e.g. NSA, Decision 11/2019 on the merits of 25 November 2019);
- an order to prohibit the processing (e.g. NSA, Decision 03/2019 on the merits of 2 April 2019);
- an order to bring the processing operation into compliance with the GDPR (e.g. NSA, Decision 07/2019 on the merits of 17 September 2019);
- an order to comply with the data subjects' requests to exercise their rights, including the right of access and the right to information (e.g. NSA, Decision 03/2019 of 28 May 2019), the right to be forgotten (e.g. NSA, Decision 06/2019 of 17 September 2019) and the right to rectification (e.g. NSA, Decision No. 01/2019 of 15 May 2019); and
- administrative fines (e.g. NSA, Decision 12/2019 on the merits of 17 December 2019 (15,000 euro)).[67]

Article 221(2) Framework Act provides that no administrative fines can be imposed on public authorities. However, a request for annulment of this article is currently pending before the Constitutional Court in a case initiated by the Federation of Enterprises.[68]

In addition to the administrative sanctions provided for by the GDPR, the Belgian legislator has introduced criminal sanctions in the form of *inter alia* fines ranging from 100 euro to 30,000 euro (to be increased with a multiplication factor of 8), which vary

65 NSA, 'Plan Stratégique 2019-2025', www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_2019-2025.pdf, pp. 20-21.

66 See arts 95 and 100 NSA Act.

67 In three cases, the NSA's decision was challenged before the Market Court in Brussels. In one particular case, the Market Court decided to annul the NSA's Decision 05/2019 on the merits of 9 July 2019 on grounds of lack of reasoning and excess of power.

68 CC, No. 7135.

depending on the nature of the infringement of the GDPR and/or the Framework Act.[69] Contrary to administrative fines, these criminal sanctions can be imposed on public authorities.

Question 12

If a data subject suffers damage as a result of unlawful processing of his personal data, he can claim compensation.[70] In many cases damage resulting from infringements of data protection law will consist of moral damage.[71] Compensation for moral damage can be granted in kind (e.g. by the publication of the judgment), but a judge may also award a pecuniary compensation.[72]

Moral damage is difficult to assess by its nature.[73] There are no standard rates for estimating the damage.[74] Most judges estimate the moral damage *ex aequo et bono*, with amounts ranging from a symbolic compensation of 1 euro to amounts varying from 500 to 1,250 euro.[75] Legal costs will often outweigh the benefit that can be gained from a claim for compensation, resulting in little case law on the matter.[76] In a rare published case of 2015, the court awarded a compensation of 750 euro, estimated *ex aequo et bono*, to an employee whose employer had installed a track-and-trace system in his company car allowing the employer to follow every movement of the employee (even outside working hours) without sufficiently informing the employee.[77] We are not aware of similar judgments since the entry into force of the GDPR.

69 Art. 222-230 Framework Act.

70 Art. 216 Framework Act.

71 Y. S. Van Der Sype and A. Vedder, 'Privacy, werk en internet of things', Or, No. 5, 2016, p. 124; FRA, 'Access to data protection remedies in EU Member States', Luxembourg, 2013, p. 28.

72 J. Van de Voorde, 'L'excuse contrainte par justice (l'amende honorable) en droit de la responsabilité belge: Recherches sur la réparation ou la satisfaction du dommage moral', RGAR, No. 2, 2019, p. 15545; E. Verjans, 'Buitencontractuele aansprakelijkheid voor schending van persoonlijkheidsrechten', RW, No. 14, 2013, p. 533.

73 E. Guldix and A. Wylleman, 'De positie en de handhaving van persoonlijkheidsrechten in het Belgische privaatrecht', TPR, No. 4, 1999, p. 1652.

74 A. Hallemans and K. Vranckaert, 'Aansprakelijkheid onder de Algemene Verordening Gegevensbescherming', TTP, No. 2, 2018, p. 11.

75 Verjans, 2013, p. 535.

76 Van Der Sype e.a., 2016, p. 124.

77 Labour court Antwerp 13 February 2015, Soc. Kron., 2015, No. 1, p. 18.

Question 13

A data subject has a right to instruct a non-profit body to file a complaint and to introduce administrative or judicial proceedings before the NSA and the judiciary on his behalf.[78] Possibilities for collective redress for data protection infringements already existed under Belgian law before the entry into force of the GDPR.[79] Groups of consumers and SMEs can be represented by non-profit organisations or public bodies to bring actions to seek collective redress for alleged violations of data protection law.[80]

One recent class action is pending before the Brussels commercial court in the wake of Facebook's Cambridge Analytica scandal.[81]

NGOs, such as the League for Human Rights ("Liga voor Mensenrechten"), put pressure on governments to increase respect for human rights by initiating proceedings before the Constitutional Court and the Council of State. Together with its French counterpart ("Ligue des Droits Humains"), the League for Human Rights has lodged an appeal before the Constitutional Court against an act that embeds fingerprint in new identity cards and against an act holding data retention obligations (see Question 15 below).[82] Also the "Ligue des Droits Humains" has recently filed a complaint demanding the NSA to launch an investigation into the alleged illegal techniques for mass collection of (sensitive) personal data used by the behavioral advertising industry.[83]

Another foundation, 'The Ministry of Privacy', is fighting against the use of fingerprints on identity cards before the Constitutional Court.[84] On 28 January 2020, the foundation announced more actions against *inter alia* the use of ANPR cameras in public, smart electricity meters and smart cities.[85]

Question 14

The NSA is obliged to carry out its tasks in a spirit of dialogue and consultation with all public and private actors involved in the protection of fundamental rights and freedoms of natural persons with regard to processing of personal data and involved in consumer

78 Art. 220(1) Framework Act.

79 G. Renier, 'L'action en réparation collective en matière de données personnelles après une année d'application du RGPD', DCCR, No. 1, 2019, p. 156.

80 Art. XVII.37, 10°/1 Code of Economic Law.

81 Test-Achats, 'Action collective Facebook', www.test-achats.be/actions-collectives/facebook.

82 CC, No. 7203.

83 Ligue des Droits Humains, 'La Ligue des Droits Humains et 13 ONG en Europe déposent plainte contre les techniques illégales de publicité en ligne', www.liguedh.be/la-ligue-des-droits-humains-et-13-ong-en-europe-deposent-plainte-contre-les-techniques-illegales-de-publicite-en-ligne/.

84 CC, No. 7150.

85 See for more information: www.ministryofprivacy.eu/ (in Dutch).

protection.[86] The NSA may be assisted by, or act at the request of, other public authorities.[87] In order to achieve cooperation, the NSA may establish committees.[88] The NSA can carry out public enquiries or consultations (such as the recent consultation regarding direct marketing) in other sectors in order to formulate opinions and recommendations that serve the interests of data protection.[89]

In the coming years, it is the NSA's ambition to collaborate more effectively with other national and regional players through cooperation agreements and thus to have a broader view than just the strict privacy landscape.[90]

D Data Processing for National Security Purposes

Question 15

The Belgian Constitutional Court has eagerly applied the EU Charter in its data retention judgments preceding and following the Tele2/Watson-judgment of the CJEU.[91]

Quoting extensively the CJEU's Digital rights-judgment,[92] the Constitutional Court considered in 2015 that the Belgian Act of 30 July 2013 on electronic communications that transposed the Data Retention Directive (hereinafter "2013 Act"), contained the same flaws and held that the 2013 Act violated articles 7 and 8 EU Charter.[93]

Following the annulment of the 2013 Act, the Belgian legislator introduced a new act in 2016.[94] This new act imposed more safeguards for retention and more limitations to access to data, but nevertheless introduced again a general blanket data retention obligation with no differentiation *ratione personae*, *rationae materiae* or *ratione temporis*. Seven

86 Art. 52(1, first section NSA Act.

87 Art. 52(1), second section NSA Act.

88 Art. 53(1) NSA Act; Preparatory works NSA Act, p. 37.

89 Art. 52(2) NSA Act. On 10 February 2020, the NSA published its new guidelines on direct marketing: NSA, Recommendation no. 01/2020 of 17 January 2020, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Recommandation_01-2020_marketing_direct.pdf.

90 NSA, 'Plan Stratégique 2019-2025', www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_2019-2025.pdf, pp. 29-30.

91 Judgment of 21 December 2016 in Joint Cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewi (Tele2 and Watson), [2016] ECLI:EU:C:2016:970 (hereinafter "the Tele2/Watson-judgment").

92 Joint Cases C-293/12 and C-594/12, Digital rights, [2014] ECLI:EU:C:2014:238 (hereinafter "Digital Rights-judgment").

93 CC 11 June 2015, No. 84/2015, in particular Rec. B.11.

94 Act of 29 May 2016 on the collection and retention of data in the electronic communications sector (hereinafter "2016 Act").

months after the adoption of this Act, the CJEU rendered its Tele2/Watson-judgment, setting new criteria for data retention obligations.[95]

A new series of requests before the Constitutional Court seeking the annulment of the 2016 Act followed after said judgment.[96] In its preliminary ruling of 19 July 2018, the Constitutional Court decided to stay its decision and ask three preliminary questions to the CJEU, summarized below:[97]

1. Must article 15(1) of Directive 2002/58/EC, read in conjunction with article 6 Charter and articles 7, 8 and 52(1) Charter, be interpreted as precluding national legislation such as that at issue, which lays down a blanket data retention obligation for national legislation whose objective is not only the investigation, detection and prosecution of serious criminal offences but also the safeguarding of national security, the defence of the territory and of public security, the investigation, detection and prosecution of offences other than serious crime or the prevention of the prohibited use of electronic communication systems, or the attainment of another objective identified by article 23(1) GDPR and which, furthermore, is subject to specific guarantees in that legislation in terms of data retention and access to those data?
2. Must article 15(1) of Directive 2002/58/EC, in conjunction with articles 4, 7, 8, 11 and 52(1) Charter be interpreted as precluding national legislation such as that at issue, which lays down a general data retention obligation if the object of that legislation is, in particular, to comply with the positive obligations borne by the authority under articles 4 and 8 Charter, consisting in providing for a legal framework which allows the effective criminal investigation and the effective punishment of sexual abuse of minors and which permits the effective identification of the perpetrator of the offence, even where electronic communications systems are used?
3. If, on the basis of the answers to the first or the second question, the Constitutional Court should conclude that the contested law fails to fulfil one or more obligations arising under the provisions referred to in these questions, might it maintain on a temporary basis the effects of the 2016 Act in order to avoid legal uncertainty and to enable the data previously collected and retained to continue to be used for the objectives pursued by the law?[98]

---

95 Case 203/15 and 698/15, Tele2 and Watson, Rec. 106-111; G. Formici, 'ECJ, the floor is yours! The never ending story between Data Retention and Right to Privacy', 28 March 2019, www.law.kuleuven.be/citip/blog/ecj-the-floor-is-yours-the-never-ending-story-between-data-retention-and-right-to-privacy/.

96 CC, Nos. 6590, 6597, 6599 and 6601.

97 CC 19 July 2018, No. 96/2018, Rec. B.21 and B.24. F. Verbruggen, S. Royer and H. Severijns, 'Reconsidering the blanked-data-retention-taboo, for human rights' sake? Belgian Constitutional Court offers CJEU chance to explain its puzzling Tele2 Sverige AB-decision', 1 October 2018, www.europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

98 Request for a preliminary ruling from the Belgian Constitutional Court of 19 July 2018, Case C-520/18 Ordre des barreaux francophones and germanophone and Others.

On 15 January 2020, the Advocate General delivered his opinion on the preliminary questions and answered the first two questions affirmatively while leaving room under the third question for the national courts to decide on the consequences of data retained under annulled legislation.[99] It is now up to the Court of Justice to decide.

99 Opinion of Advocate General Campos Sánchez-Bordona in Case 520/18, Ordre des barreaux francophones and germanophone and Others, ECLI:EU:C:2020:7.

Bulgaria

Ana Velkova[*]

Bulgaria has had a Personal Data Protection Act (PDPA) since 2002, even before Bulgaria joined the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (The Convention No 108).

Our legislation has put serious requirements for lawfulness in data processing, protection of the data and not using personal data information when the purpose of the processing could be reached without it.

Both the PDPA and practice of the national supervising authority (Commission for Personal Data Protection, hereinafter CPDP) and of the courts also follow the main principles of personal data protection laid down in Directive (EC) 95/46 and in the General Data Protection Regulation (hereinafter "GDPR") nowadays. The national legislator has chosen to consolidate in one act those of the items of the GDPR where a nation approach is required and the text of Directive (EC) 2016/680.

A Setting the Scene

Question 1

1.1.

Our PDPA does not deviate from the European Commission guidance on direct application of the GDPR and its reconciliation with the issues which the GDPR leaves to the discretion of and legal solution offered by each Member State.[1] Following that the national legislator adapts the existing law to the new requirements of the GDPR. First of all, the redundant provisions as well as those which were not in compliance with the GDPR have been removed.

The national legislator accepts the progressive approach to complying with EU data protection legislation by including the GDPR concept and the rules of Directive (EC)

* Partner at Simeonov & Dermendjiev Law Firm with practice areas on arbitration, administrative and civil litigation, regulatory matters in data protection, ecology, aviation, sports, public procurement, EU law.

1 PDPA in English: https://www.cpdp.bg/en/index.php?p=element&aid=1194. All webpages referred to were visited 1 February 2020.

2016/280[2] in one common legal act. Despite the difference between the legal nature of both EU law acts, Regulation and Directive, such approach is logical and successful in principle, as well as referring to legislative technique philosophy. To gather in one single legal act the common data protection rules and to underline the specific requirements because of the nature of the processes referred to in Directive (EC) 2016/680 seems as codifying the national legal framework in the field of protection of individuals with regard to data processing.

1.2.

1.2.1.
The first group of national legal instruments concerns the issues where the GDPR gives the opportunity to or requires a Member State to create its national solutions. Such spheres are:

1.2.1.1.
Rules on processing of national identification number:

Actually, the personal identification number which was created as a really unique mark to identify any person and includes in itself information about date of birth, area of origin and gender, is one of the least secret personal data in our daily life. Especially if one is an active person who is a partner in a company, possesses real estates, etc. So much so that in 2018, a discussion about the personal identification number not to be the only means of identifying the user started. Nowadays, the PDPA permits an information containing personal identification number to be available only if a special law explicitly requires public access to it. Otherwise, the controllers providing services by electronic means are required to take appropriate technical and organisational measures to ensure that the personal identification number is not the only means of identifying the user (in this sense: article 25g § 2 PDPA).

1.2.1.2.
Data processing for journalistic purposes and for the purposes of academic, artistic or literary expression: the PDPA requires the freedom of expression and the right to information to respect the data subject privacy.

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ 119/89.

In order to boost finding of "the golden mean", the national legislator has put several criteria on the basis of which the evaluation if the relevant data processing has a real value for the society should be done, e.g. is it of public interest or it is just a piece of information which is interesting for the members of the public, i.e. it has the characteristics of gossip.

The criteria will be further analysed when answering Question No 8.

1.2.1.3.

Certain aspects of data processing by employers/appointing authorities: the legal instruments applied in this area intend to reach the balance between the legitimate interest of employers or appointing authorities and the fundamental rights and freedom of employees. The principle adopted by the legislator is that employees should be informed about each of the measures/systems/organization which are applied by the employer or appointing authority in favor of their legitimate interest which should not exceed the nature of the activity, special needs and available resources of the enterprises.

There are special rules concerning collecting, storing and returning and/or erasing or destroying the originals or notary certified copies of any documents candidates are requested to submit in staff selection procedures. The storage period is limited to six months unless the applicant has given consent for a longer period of storage.

When the period of time expires, the employer or appointing authority shall erase or destroy the documents containing personal data unless otherwise provided for by a special law.

1.2.1.4.

Despite the GDPR principle being inapplicable to the deceased persons' data, the national legislator has provided for rules regarding the processing of personal data of deceased persons. PDPA requires a legal basis for the deceased persons' data processing and the controllers or processors are obliged to take the appropriate measures so that the rights and freedoms of others or a public interest should not be adversely affected. The persons authorized to get access to personal data of a deceased person, including by providing a copy, are the heirs of the person or other persons with a legitimate interest.

1.2.1.5.

Data processing for National Archiving Fund purposes is found as processing in public interest and articles 15, 16, 18, 19, 20 and 21 GDPR and shall not apply in such cases (that exception is under article 25k of PDPA).

In the case where personal data is processed for statistical purposes, articles 15, 16, 18 and 21 GDPR shall not apply.[3]

3 Art. 25l PDPA.

1.2.1.6.

The national legislator finds data processing for humanitarian purposes as lawful in case it is operated by public bodies or humanitarian organisations, as well as when processing concerns cases of disaster within the meaning of the Disaster Protection Act.[4]

In the case of such processing purposes articles 12-21 and article 34 of GDPR are not applicable.

1.2.1.7.

Obligations in large-scale processing are seen in article 25e of PDPA:

The data controller or processor shall adopt and apply rules for large scale personal data processing or for a large scale systematic monitoring of publicly accessible areas, including video surveillance, if the controller or processor implements appropriate technical and organisational measures for safeguarding the rights and freedoms of data subjects. The rules on large scale systematic monitoring of publicly accessible areas shall state the legal grounds for setting up a monitoring system, its scope and means, storage period of the information records and their erasure, the individuals' right of access, the provision of information to the public about the monitoring, as well as restrictions with regard to the access of third parties.

In paragraph 2 of the same article, the national legislator obliges the National Supervisory Authority (hereinafter "NSA") to issue guidelines to data controllers and processors for the performance of the obligations detailed above and make them available on the NSA internet site.

PDPA says that

> *"Large-scale (processing operations) shall be monitoring and/or processing of personal data of a significant or unlimited number of data subjects or amount of personal data, where the core activities of the controller or the processor, including the means by which these activities are carried out, consist of such operations".*

1.3.

The second group of specific national legal solutions concerns the restrictions permitted under article 23 of the GDPR: the way and the terms to execute the rights under articles 15-22 of the GDPR.

4 https://www.lex.bg/laws/ldoc/2135540282.

1.4.
The third group of legal instruments concerns the transition of Directive (EC) 2016/680. There are certain differences in the principles adopted by the Directive. For example, the principle of transparency is not the leading one in the case of data processing for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. The storage period regarding those data differs also from the period for storage of personal data in the case of regular processing.

Question 2

Actually, even now the Charter is a certain exotic instrument in comparison with the European Convention on Human Right (hereinafter "ECHR"). As far as the Convention is an international legal instrument it is easy to find the spot of its application. But the Charter of Fundamental Rights of the European Union (hereinafter "Charter) supposes to be of limited application (only within the scope of EU law), so our national legislator does not make very deep differentiation between the "respect for private and family life" (article 7 of the Charter) and "personal data protection" (article 8) as far as the understanding of the national law is that the institute of "personal data" includes the privacy of the personal and family relationships.

So, our national legislation and practice accept and rely on the common, GDPR's, principles and rules for personal data protection and our national law on the PDPA does not include any special provision to respect private and family life. On the other hand, private and family life privacy is stated to be one of the criteria in search for the balance between the freedom of expression and the right to information and the right of personal data protection in article 25h of Personal Data Protection Act. In article 25h, paragraph 2, item 2, the national legislator requires that "the impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation" has to be evaluated searching for the balance aforementioned.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

3.1.
The national jurisprudence and the practice of the NSA usually interpret those principles in the most common way, as it is required by the EU law and the case law of the Court of

Justice of the European Union. The understanding of the NSA and the courts for an eventual difference or nuance in the interpretation, could by noticed when the requirements of the basic principles of the PDPA should be applied together with the requirements of other special laws as Anti-money Laundering Measures Act, etc. when even the purpose of data processing is different, the controller has the obligation to collect more data because it fulfils its obligation under that law.

Other examples are Occupational Health Authorities, who maintain health records by virtue of their own regulations and not because they have been assigned to do so by the administrator.

The NSA follows the same philosophy in its Opinion on the Draft of the Protection and Development of Culture Act where the NSA finds that collecting data of young people beneficiaries of E-cards for cultural activities is a fair processing: after the law adoption such collection will be based on the controller's (Ministry of Culture) legitimate interest or its legal obligation (it depends on the point of view).[5]

3.2.

The constant practice of the NSA calls for a minimalist approach to the use of personal data, especially the data of those individuals who are not public persons and have no direct relation on a debate of public interest. The exception to allowing deviations from such an approach is when that approach would impede the exercise of the right to information.[6]

Question 4

4.1.

Obviously, the controllers find the "consent" of the data subject as one of the most easily obtainable reasons for data processing. Many of them put themselves in the stalemate of not obtaining the consent requested (by the subject) and thus unable to process the data lawfully, although there are other grounds for processing for the same purpose for which they requested consent. In order to avoid that Catch 22 the NSA has published Guidelines where the situations when consent should not be required are pointed out and explained in detail.[7] Those Guidelines were published after 25 May 2018 and up to that moment quite few controllers had already got in the position waiting for data subject consent, which will probably never come.

5 That NSA Decision (unfortunately, all NSA documents are only in Bulgarian) is published on: https://www.cpdp.bg/index.php?p=element_view&aid=2085.

6 NSA Decision: https://www.cpdp.bg/index.php?p=element_view&aid=2186.

7 The Guidelines: https://www.cpdp.bg/?p=element_view&aid=2117.

So, from a formal point of view, any further processing of data for the purpose for which consent was previously sought should be considered illegal, even if another ground for processing the data for the same purpose exists. The same "dead end" situation is encountered when the controller had started to process the data on the consent of the data subject although other grounds had existed and then later, the data subject decided to withdraw its consent.

It is evident that "the consent" is the most uncertain ground for data processing: the lawfulness of controllers' activities depends on the data subject's position/mood/emotions. However, the case is not this when data processing is based on the controller's "legitimate interest".

4.2.

There is no legal definition of "legitimate interest" but the courts give the following definition: in order to be recognized as "legitimate" the source and the purpose of the interest should be to satisfy a particular human need, to be admissible by the law, i.e. legal remedies are provided for its enforcement/satisfaction (subjective rights), and in case such rights are not expressively provided for, they are admissible in the light of the general principles of law.

Obviously there are cases where the legitimate interest is expressly defined by the law and the controller should not hesitate to proceed with data. But if legitimate interest does not exist by law but because of the concrete situation, then an additional evaluation is required. The court is competent to make such an evaluation. The main criteria should be whether the data processing would be in favour of revealing the objective truth, respectively to the benefit of either of the parties. A simple example of that is when at the time of court proceedings one of the parties would like to present information about the counterparty before the court, which means "personal data" and for its dissemination any consent is required. Surely, the counterparty will not give her/his consent. So, the deciding court should assess whether that information has its "added value" for the party within the frame of the process. Then the court could permit or deny the information to be obtained by the party concerned.

Specifically, in Bulgarian law, the order of receiving it officially, i.e. legally, is in article 186 of the Code of Civil Procedure, which provides for the possibility, after a positive assessment of admissibility and relevance, that the determining court issues a court certificate whereby the institution having the requested data cooperates and provides them. It should be underlined in this context that it is not enough for the controller to have the

information she wishes to present before the court or any third party at her disposal, but she needs a legal ground to disseminate that information.[8]

Question 5

Actually, there was no debate and the new PDPA does not pay any special attention to personal data processing within digital content, particularly of eventual "counter-performance".

"Counter performance" is easily visible during the process of labour contract signing. Usually, employers require a lot more personal data than they really need to hire the candidate and to prepare and sign the labour contract. An example of such unreasonable requirements whose fulfilment is a condition *sine qua non* for the employment relationship to be established are the following requirements of the employers: (i) number of personal identification card or passport although the law (Labour Code and Ordinance No 4/May 1993 for the documents necessary to sign a labour contract) requires only a personal identification number; and/or (ii) "criminal record certificate" although there is not any special law which requires such information for the position the candidate applies for; and/or (iii) the employers keep the job history book of the employees in the company's/enterprise's archive office: the job history book, being a private document of each person where all his/her jobs salaries, eventual penalties and praises are enlisted, and as such its storage should be with the holder. Neither the law nor the Ordinance require its storage with the employer but it is a "common practice" to leave it with the employer when signing the employment contract; and if the employee refuses, the employment contract could be denied by the employer, at least that was the situation before 25 May 2018.

In most of the cases such unfounded document requests are placed by the employers unwillingly, due to low levels of GDPR awareness.

Question 6

6.1.

In article 52, paragraph 1 of the national PDPA the Bulgarian legislator has accepted a wording of the presumptive ban of article 22, paragraph 1 from the GDPR which allows the data subject to be subject to a decision based solely on automated processing, including

8 The Decision on that case is Resolution No 10776 from 10.07.2019 on administrative case No 595/2018 at the inventory of Supreme Administrative Court: www.sac.government.bg/court22.nsf/d6397429a99ee2afc225661e00383a86/1a08ddde3fd74702c22584310049a706?OpenDocument.

profiling, if such does not produce *adverse* legal effects concerning him or her. Admitting this wording, the refinement "*unless this is provided for in Union law or in the legislation of the Republic of Bulgaria*" sounds lik even if potential "adverse effects" could occur, automatic data processing and profiling is acceptable if either law allows it. Surely, the characteristic "adverse" could be interpreted quite widely and in a biased way.

6.2.
In article 52, paragraph 2 of the PDPA, the national legislator has permitted an automated processing even on the special categories of personal data (article 9 GDPR) as long as suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject are in place.

6.3.
In any case, an impact assessment is required as the minimum elements of the assessment process are listed in article 64, paragraph 2 of the PDPA: (i) a general description of the envisaged processing operations; (ii) an assessment of the risks to the rights and freedoms of data subjects; (iii) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Chapter taking into account the rights and legitimate interests of data subjects and other persons concerned. Discrimination impact is prohibited in any case.[9]

6.4.
The controller and the processor are required to keep logs for at least the following processing operations: collection, alteration, consultation, disclosure including transfers, combination and erasure, so that those logs could be used to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The logs shall be used solely for the verification of the lawfulness of the processing, self-monitoring, ensuring data integrity and data security and criminal proceedings. The time limits for storage and archiving of the logs should be established by the controller or processor.[10]

6.5.
There are certain stages of automated data processing where strict control is required by the law to be applied by controller and/or processor as a measure to protect the rights and

9 Art. 52, para. 4 PDPA.
10 Art. 64 PDPA.

freedoms of natural persons. Those areas are: (i) equipment and data access (no unauthorised person access to processing equipment used for processing of personal data and/or to data not covered by the personal access authorization); (ii) data media control (authorised reading, copying, modification or removal of data media only); (iii) storage control (prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data); (iv) users control (authorised persons using data communication equipment only); (v)communication control (ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment); (vi) input control (ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input); (vii) transmit control (prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media).

6.6.
The national legislator provides that the rules of processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, safeguarding against and prevention of threats to public order and security (Charter VIII of the PDPA) must be applied in case of thoroughly or partly automatic processing and profiling (article 43 of the PDPA). One might say that such legislative approach to a certain degree remedies the deviation of article 22 GDPR conception.

Question 7

7.1.
Actually, the right to erase is a source of dispute almost only within the context of journalists' activities where it is a great challenge to find the balance between right to privacy of the personal life, freedom of expression and right to information. Unfortunately, in this case the "balance" is not a physical category and it is not concentrated in one single cross-point. Actually, it is the interest of the individuals not their rights that are the leading criterion; and sometimes it is the one who is stronger who wins, not the rightful one. Detailed considerations are given below, in item 8.

7.2.
The right of erasure is an obligation for the controller under the hypothesis of 25a of the PDPA where the data controller or the processor have been provided by with personal

data without legal basis pursuant to article 6(1) GDPR or contrary to the principles under Article 5 of the same Regulation, they shall return such data within a period of one month after having become aware of it or, if this is impossible or would involve disproportionate efforts, shall erase or destroy the data. The erasure and destruction shall be documented.

7.3.
In case of incorrect data even if the processing is for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security, the data should be rectified or erased by the controller or by the recipient in cases of data transmission.

7.4.
In case the law says nothing, the controller is competent to determine the data storage period. In case the controller decides the storage period to be extended, a special written and motivated decision should be issued.

7.5.
Even though the understanding that "the right to erase" is not an absolute right, there are enough strong sanctions in case the controller denies unreasonably to erase the data. The data controller shall maintain a record of the categories of personal data processing activities which shall contain where possible, the envisaged time limits for erasure of the different categories of data.

7.6.
The cases where the controller is obliged to erase the data are provided in article 56, paragraph 2 of the PDPA: (i) where the data collected by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security are processing other than the purpose for which that data have been originally collected; (ii) where the processing is not necessary for the exercise of powers by a competent authority for the purposes referred to in previous sentence and where such processing is not provided for in Union law or in a statutory instrument which defines the purposes of the processing and the categories of personal data which are processed.; (iii) where the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's

sex life or sexual orientation without that being strictly necessary, if there are appropriate safeguards for the rights and freedoms of the data subject, and it is provided for in Union law or in the legislation of the Republic of Bulgaria.[11]

7.7.
The controller is authorised to deny erasure of the data where this is necessary in order to (i) avoid obstructing official or legal checks, investigations or procedures; (ii) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (iii) protect public order and security; (iv) protect national security; (v) protect the rights and freedoms of others.

7.8.
The "right to erase" is almost absolute in the relations between the data controller and the data processor as the last one is obliged to erase the data if the controller requires that without the option to refuse unless the conditions and procedure for the processing are provided for in Union law or in the legislation of the Republic of Bulgaria.

7.9.
The right to erase could be executed by the NSA, respectively the Inspectorate, in exercising supervision, the supervising authorities have power to order the controller or processor to bring data processing operations into compliance with the applicable provisions, including to order the rectification, completion or erasure of personal data or restriction of the processing.

Question 8

8.1.
This is one of the most controversial matters when it comes to personal data processing. Both law and the practice are used to talk about the balance between the freedom of expression and the right to information on the one hand and the privacy of personal and family life on the other hand, as main criteria to find data processing lawful; however, everyone is quiet when it comes to the characteristics of that mythical balance.

8.2.
When it comes to Bulgarian legislation concerning data processing for journalistic purposes and for the purposes of academic, artistic or literary expression, the GDPR does not

11 Art. 51 PDPA.

influence much the main principle adopted by the Bulgarian legislator in 2002, when the PDPA was first drafted. What is novel here, is that the amendment introduces criteria on the basis of which it should be assessed if the above mentioned balance exists or not.

8.3.

The criteria under article 25h, paragraph 2 of the PDPA are as follows:

i. Nature of the personal data;
ii. The impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation;
iii. The circumstances under which the personal data became known to the controller;
iv. The character and nature of the statement under which the rights of freedom of expression are exercised;
v. The significance of the disclosure of personal data or the publishing of the data for the clarification of a matter of public interest;
vi. Taking into consideration whether the data subject occupies a position under Article 6 of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act or is a person who, because of her/his activity and public status enjoys lesser protection of her/his privacy, or whose actions impact the society;
vii. Taking into consideration whether the data subject has contributed with her/his actions for the disclosure of her/his personal data and/or of information about her/his private and family life;
viii. The purpose, content, form and consequence of the statement when the rights pursuant paragraph (1) are exercised;
ix. The compliance of the statement for exercising the rights of freedom of the expression and the right of information with the fundamental rights of citizens;
x. Other circumstances relevant to the case.

8.4.

At the moment of drafting the present report there is not any court jurisprudence on these criteria application and/or evaluation. There is not any opinion of the NSA either. But there is a Request signed by fifty members of the Parliament asking The Constitutional Court to find those criteria in contradiction to the national Constitution and ECHR. BAEL has been invited to present an opinion on this request and the position declared by our Association was one in defense of the criteria. The mainline of our position is that the information journalists make available should be really of great importance for society, for its judgments and knowledge and not just a piece of information that is interesting for the people, e.g. do not disseminate any information only because it makes the circulation of the newspaper high. There are a lot of examples in our reality of unnecessary private

details made available to the public despite those details being irrelevant to the activity and/or position of the public person the society should be informed about.

8.5.

One of the latest principal NSA opinions on these matters concerns data processing by the Prosecutor's Office of the Republic of Bulgaria when publishing press releases and providing information for journalistic purposes.

The position of the NSA is the following:

> *"The publication of personal data of accused persons in pre-trial proceedings on the websites of the prosecutor's offices, as well as their provision to the media for journalistic purposes, is lawful when there is a legal obligation or there is an overriding public interest". In cases where for the public purpose it is impossible or inappropriate to publish the information in an anonymous or pseudonymized form, then the indication of the name, position or place of work of the accused would be sufficient to achieve public awareness, and the publication of a personal identification number and any relations with third parties who are out of the process, etc. would be excessive. As a general rule, the personal data of other participants in pre-trial proceedings, such as witnesses, experts or related to these categories of third parties, etc., should not be published or otherwise disclosed, as long as there is no legal obligation to do so or overriding public interest. An exception could be made with respect to persons holding high public positions within the meaning of Art. 6 of the Anti-Corruption Law and the Forfeiture of Illegally Acquired Property or another Person, which by its nature has an effect on the public, or where the publication of the information protects the vital interests of the data subject. In all cases of publishing personal data of participants in pre-trial proceedings or providing them to the media, the principles for processing personal data in Art. 5 of Regulation (EU) 2016/679, in particular the principles of minimizing data in order to achieve the objective, accuracy of data and limitation of storage time, should be applied."*[12]

Though this is one of the most specific and detailed opinions of the NSA referred to data processing for journalistic purposes, it uses general expressions as "overriding public interest" and "effect on the public" which leave the final evaluation in the hands and conscious of the author of the press release.

12 Opinion of CPDP No НДМСПО–01-502/26.06.2018г. https://www.cpdp.bg/index.php?p=element_view&aid=21161.

8.6.

The national legislator provides for the following exemptions under article 85, paragraph 2 GDPR: articles 6, 9, 10, 30, 34 and Chapter V of Regulation (EU) 2016/679. Another exemption is that of article 25c the PDPA. Actually, this provision concerns the rights of data subjects under the age of 14 and requires the administrator to make sure that consent for data processing from the parent with parental rights or by a legal guardian is given. So, by this provision even the privacy of a little child could be less important than the freedom of expression and right of information. This report finds that exemption excessive and unfair. Even though the place of the following comment is misplaced, the national legislative decision that only persons below 14 are to be considered "children" is at least strange having in mind that according to our national law persons up to 14 years old are infants, between 14 and 18 are minors (and their civil rights continue to be exercised with parental consent) and only after 18 do they receive full rights. So, the legal decision not to require parental consent for data processing concerning children of all ages for journalistic purposes is not safe for children and for their future as a whole.

8.7.

Where data processing is for journalistic purposes and for the purposes of academic, artistic or literary expression, the data controller or processor may deny the data subjects, fully or partially the exercise of the rights pursuant articles 12-21 GDPR.[13]

8.8.

The autonomy of data processing for journalistic purposes and for the purposes of academic, artistic or literary expression, is fully protected with the provision of paragraph 4 of article 25h the PDPA: *"the exercise of the powers of NSA pursuant to Article 58 (1) of Regulation (EU) 2016/679 shall not affect the secrecy of information sources"*.

8.9.

Another group of exemptions are provided for by the national legislator where personal data are processed for the purposes of creating a photographic or audio-visual work by means of capturing the image of a person in the course of the public activity or in a public place: in those cases article 6, articles 12-21, and articles 30-34 GDPR.

13 Art. 25h, para. 3, point 2 PDPA.

C Domestic Enforcement of Data Protection Law

Question 9

9.1.

9.1.1.
The national supervisory authority is the Commission for Personal Data Protection (CPDP). It is created as independent supervisory authority which protects the individuals with regard to processing of their personal data and access to these data, as well as the supervision on the compliance with Regulation (EU) 2016/679 and with national legislation. Surely, the CPCP provides assistance with the implementation of the state policy in the personal data protection field.

9.1.2.
There is an "alternative" supervising authority provided for in the PDPA - the Inspectorate of the Supreme Judicial Council (The Inspectorate) – which exercises supervision and ensures compliance with Regulation (EU) 2016/679, with the PDPA and with the statutory instruments in the field of personal data protection upon the processing of personal data by the courts when acting in their judicial capacity and by the prosecution and the investigating authorities when acting in the judicial capacity for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. Where the courts and the prosecutor's office and the investigation's office act as employer the competent supervising authority is the CPDP.

9.2.
The CPDP consists of a Chairperson and four members who are elected by the National Assembly after a nomination by the Council of Ministers for a five-year term and may be elected for one more term. The Commission adopts decisions by a majority of the total number of its members. The meetings of the Commission are open to the public. The Commission may decide to hold closed meetings. The CPDP reports its activity to the National Assembly by 31st March each year.

Eligible to be members of the Commission are Bulgarian citizens who hold a university degree in information science or in law or hold a master's degree in information technology and have not less than ten years working experience. Surely, the candidates should not been sentenced and/or have conflict of interests working another job instead of scientific research or teaching. A qualified lawyer who meets the requirements under Paragraphs (1) and (2)is elected chairperson of the Commission.

9.3.

The Commission fulfils the tasks pursuant to Article 57 of Regulation (EU) 2016/679. Other duties of the CPDP are to analyse and exercise supervision and to ensure compliance with Regulation (EU) 2016/679, with PDPA and with the statutory instruments in the personal data protection field, except for the cases which concern issues within the framework of Directive (EC) 2016/680 (in which the Inspectorate with Supreme Judicial Council is the competent supervisory authority). The CPDP is competent to issue secondary legislation acts in the personal data protection field, including instructions, guidelines, recommendations and best practices in connection with personal data protection. The CPDP ensures the implementation of the decisions of the European Commission in the personal data protection field and the implementation of the legally binding decisions of the European Data Protection Board under article 65 GDPR also. The CPDP participates in international cooperation with other personal data protection authorities and international organisations on personal data protection issues and in the negotiations and the conclusion of bilateral or multilateral agreements on matters within its competence. The CPDP is competent to organise, coordinate and provide personal data protection training.

Surely, the CPDP is the competent body to exercise the powers pursuant to Article 58 of Regulation (EU) 2016/679.

9.4.

9.4.1.

The Chairperson and the members of the CPDP exercises control by means of prior consultation, inspections and joint operations in compliance with Regulation 2016/679 and with PDPA, especially in cases where data are processed for the performance of a task carried out in public interest, including processing in relation to social protection and public health. In such a case, the CPCD may authorise the processing before the period referred to Article 36 (2) of Regulation (EU) 2016/679 expires. The prior consultation shall take place pursuant Article 36 (2) and (3) of Regulation (EU) 2016/679.

Inspections will be conducted on the initiative of the CPDP, at the request of stakeholders, or after an alert has been submitted. Where there is a need, any expert opinion is allowed.

9.4.2.

The CPDP conducts accreditation of certification bodies in pursuant Regulation (EU) 2016/679 on the basis of the requirements laid down by the CPCD or by the European Data Protection Board. The accreditation is issued in accordance with Article 43 (2) of Regulation (EU) 2016/679 for a period of five years and may be renewed. The certification

criteria, mechanisms and procedures, seals and marks are laid down in an Ordinance adopted by the CPDP. The Ordinance shall be promulgated in the *State Gazette*. As of September 2019 no such Ordinance has been issued.

9.4.3.
The CPDP approves codes of conduct by sector and field of action pursuant to Article 40 of Regulation (EU) 2016/679. Bodies for monitoring the codes of conduct will be authorised by the CPDP, with compliance of Article 41 of Regulation (EU) 2016/679.

9.5.

9.5.1.
The CPDP maintains the following public registers: (i) of data controllers and processors which have designated data protection officers; (ii) of accredited certification bodies; (iii) of codes of conduct pursuant Article 40 of Regulation (EU) 2016/679.

9.5.2.
The following registers maintained by the CPDP are not public: (i) of the infringements of Regulation (EU) 2016/679 and the PDPA, as well as of the measures taken in accordance with the exercise of the powers referred to in Article 58 (2) of Regulation (EU) 2016/679; and the (ii) register of the notifications of personal data breaches under Article 33 of Regulation (EU) 2016/679.

9.6.
The CPDP is a state budget financed legal person. Its Chairperson is a first level spender which means that the President of the CPDP is authorised to spend the money at its own discretion but within the frames laid down by the law. For example, there are special law provisions on how the monthly remuneration of the Chairperson and the CPDP members should be formed: the members of the Commission shall receive basic monthly remuneration equivalent to 2.5 average monthly wages received under labour and civil service contract in accordance with the information provided by the National Statistical Institute as the basic monthly remuneration shall be recalculated every three months, taking into consideration the average monthly wage for the previous three months. The Chairperson of the Commission shall receive a monthly remuneration which is 30 per cent higher than the basic monthly remuneration of the members of the CPDP. Up to September 2019 the officially declared (by National Statistical Institute) average remuneration is BGN 1253 or EUR 637.

The CPDP has its own income, different from the state budget funds. Such are the fees charged for the training organized by the CPDP and certificates issued, the income of the

fines imposed by the CPDP and upheld by the court, European Union financing programmes and projects, etc.

Question 10

10.1.

In cases of infringement of their rights pursuant the GDPR and the national PDPA, the data subjects shall have the right to bring the infringement before the NSA (both the CPDP or The Inspectorate) within six months after having become aware of the infringement but no later than two years after.

The NSA shall inform the complainant of the progress of the complaint or of the result within three months after the infringement has been brought to the attention of it. This way there is not a dead line in which the NSA shall issue its decision. So, it supposes such a term should be reasonable.

10.2.

The decision issued by NSA may apply the measures referred to in points (a) to (h) and (j) of Article 58 (2) of Regulation (EU) 2016/679 or in Items 3, 4 and 5 of Article 80 (1) and, in addition to or instead of them, the NSA may impose an administrative fine in accordance with Article 83 of Regulation (EU) 2016/679 and under the PDPA.

Where the complaint is obviously unfounded or excessive, the NSA may adopt a decision to dismiss the complaint.

The decision of the NSA is subject to appeal pursuant to the Administrative Procedure Code within 14 days of receipt.

10.3.

The complaint to the Commission may be submitted by a letter, fax or by electronic means under the procedure of the Electronic Document and Electronic Trust Services Act. No action shall be taken on anonymous complaints and on complaints which are not signed by the complainant or by a legal or authorised representative.

It is not obligatory to bring the infringement before the NSA: the data subject may appeal against any actions or acts of the data controller and processor directly before the court pursuant to the Administrative Procedure Code.

The court is the only competent body to decide on compensation for the damage suffered as a result of an unlawful processing of personal data from the data controller or processor. The NSA is not authorised to issue decisions on that matter. So, if the data subject decides to bring her or his claim to the court directly, actually she or he saves time and procedural efforts.

But once proceedings before the NSA have been started, the data subject may not bring a violation to the attention of the court.

10.4.
Where a decision to implement a binding decision of the European Data Protection Board is required to be adopted, Articles 263 and 267 of the TFEU shall apply accordingly.

Question 11

11.1.
There are no special additional sanctions adopted by the Bulgarian PDPA than fines and compulsory measures provided by the GDPR.

The measures referred to in article 58 items (a) to (g) and (j) of the GDPR and the measures referred to in article 80 (1) items 3, 4 and 5 are applicable to any violation of personal data protection. The specific measure, surely, depends on the background of the case in question and on the Commission's evaluation about the facts and their impact.

11.2.
The national legislator differentiates the infringements which are subject to administrative fines or pecuniary sanction according to article 83, paragraphs 4 and 5 from certain other infringements which will be subject to a much lower fine that those in the GDPR (article 86 the PDPA: the size of the fine or pecuniary sanction is no more than BGN 5000, e.g. a bit more than EUR 2 500).

Even though the PDPA does not provide it explicitly, the practice of the NSA shows that very often only a fine/pecuniary sanction or only a compulsory administrative measure (those under article 58, paragraph 2) is imposed by the Commission.

11.3.
According to the Rules on the activity of the Commission, adopted in August 2019, the compulsory administrative measures under article 58 paragraph 2, article 80, paragraph 1, point 3, 4 and 5 shall apply to: (i) consideration of a complaint against a personal data controller under article 38 of the PDPA; (ii) carrying out the control activity of the Commission under article 12 of the PDPA including and when a signal is received; (ii) supervision of the commission under article 34, paragraph 4, article 42, paragraph 7, second sentence and article 43 GDPR.

Question 12

By the beginning of this century the national jurisprudence strictly followed the understanding that intangible harm is inherent only to individuals. Only in the last five–six years have the courts timidly started to recognize legal entities as entitled to bear intangible harms. But in both cases, individuals and legal entities, the intangible harms are calculated by the court only on the basis of "inner conviction" of the judge-rapporteur or of the panel. *"Inner conviction"* is one of the basic principles in making the decision according to our national law (art. 12 of Civil Procedure Code).

There is not any methodology whatsoever, neither in a public legal act nor in any document meant for internal use of the judges to establish evaluation criteria. In a common mode the witnesses are those who "decide" the case: the only source of information about the emotions and negative consequences passed by the claimant are their (witnesses') statements. Usually, in such proceedings, only the claimant is allowed to summon witnesses about her/his emotions and non-material consequences resulting from the wrong harmful activity of the respondent.

Surely, the first step is to assert that there is something illegal done by the respondent. But once that fact is proved, the information of the possible harms comes from the witnesses. The Respondent witnesses are not allowed because of the understanding (the principle) that "the negative claims are not subject of proof". This way the respondent is deprived of the opportunity to rebut the testimonies of the claimant witnesses by other witnesses' testimony; the only step the respondent could rely on is the cross-examination.

Question 13

13.1.

Nowadays, there are no peculiar activities or role of NGO's in the data protection process and/or data subject representations.

Anyway, in article 83 of the PDPA the national legislator accepts the concept of article 80 of GDPR and provides the data subjects the right to mandate a not-for-profit legal person, which has statutory objectives which are in the public interest and is active in the field of protection of the rights and freedoms of natural persons with regard to the protection of their personal data, to lodge a complaint on her/his behalf and to exercise data subject rights. Such authorization does not concern the data subject right to receive compensation. With regards to the exercise of that right, the data subject may not mandate any other person or structure aforementioned.

13.2.

There are certain presumptions in the PDPA when the data subject may exercise one's rights through the NSA or, respectively, through the Inspectorate. In such cases, the Commission or, respectively, the Inspectorate, shall verify the lawfulness of the refusal (article 57, paragraph 1of the PDPA).

Such presumptions are the following:

i. if the controller delays or refuses, in whole or in part, the provision of the information for processing grounds, storage period or criteria about it, which are the potential recipients of the data and/or other additional information, with the excuse that its delay or refusal is in order to avoid obstructing official or legal checks, investigations or procedures, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protect public order and national security and/or protect the rights and freedoms of others;
ii. if the controller restricts the access of the data subject to the data and information which concerns her or him and those data are under process with that controller, without any or with ungrounded explanation about such restriction;
iii. if the controller refuses to proceed with rectification, completion, erasure or restriction of the processing of personal data because of any of the reasons in point (i) above or fails to inform the data subject about the refusal grounded on the same reasons.

In those cases, the NSA or, respectively, the Inspectorate, shall inform the data subject that at least all necessary verifications or consultations have taken place and of the right of the data subject to seek a judicial remedy.[14]

Question 14

The NSA regulates its activity, the activity of its administration, as well as administrative proceedings with Rules of Procedure promulgated in the *State Gazette.* (article 9, paragraph 2 of the PDPA). In those Rules (article 14), in exercising its powers, the NSA is authorized and obliged to cooperate with state bodies and non-governmental organizations by participation in meetings of working groups, holding working meetings, carrying out joint activities, including inspections, implementation of joint projects and drafting regulatory acts. In the course of relations with other bodies and organizations, the NSA may conclude cooperation and mutual assistance agreements. Nowadays, the NSA has a very active cooperation with international structures such as Joint Supervisory Bodies and Working

14 Art. 57, para. 2 PDPA.

Parties to the EU Council and Data Protection Groups to the European Data Protection Supervisor.

D Data Processing for National Security Purposes

Question 15

There is an explicit definition on "national security" in Bulgarian legislation. Article 2 of the law for the management and operation of the national security system says:

> *"national security is a dynamic state of society and the state, while protecting the territorial integrity, sovereignty and constitutionally established order of the country, when the democratic functioning of the institutions and fundamental rights and freedoms of the citizens are guaranteed, as a result of which the nation preserves and increases its well-being and develops and when the country successfully defends its national interests and realizes its national priorities".*

This definition is applied to all the national laws which concern the national security though in different aspects: "National Security" Directorate Act, Classified Information Act, Special Intelligence Law, etc.

Practically, as of March 2015 when the Constitutional Court has repealed in whole the provisions of the Electronic Communication Act which had treated the obligation of the enterprises providing electronic communication services to store the traffic for a period of 12 months, our legislation provides for the unconditional application of article 7 and 8 of the Charter, at least as regards the information that can be obtained from the electronic communications of any individual.

Where any information is required for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, a special permission should be issued by the court under the procedure of the Special Intelligence Act after a request by the competent authority: prosecutor's or investigator's offices.

Croatia

Antonija Ivančan[*]

A Setting the Scene

Question 1

Following the enactment of the General Data Protection Regulation (hereinafter "GDPR"),[1] the main national legal instrument enacted for the enforcement is Zakon o provedbi Opće uredbe o zaštiti podataka (the Act on the implementation of the General Data Protection Regulation, hereinafter "GDPR Implementing Act"),[2] which has set aside the previous Personal Data Protection Act (Zakon o zaštiti osobnih podataka).[3] However, it must be noted that the Act, pursuant to its article 1(2), does not apply to personal data processing for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. That processing has been regulated by the Act on protection of physical persons with respect to processing and exchange of personal data for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija)[4] which was enacted to implement Directive (EU) 2016/680.[5]

---

* University of Zagreb, Department of EU Law.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Zakon o provedbi Opće uredbe o zaštiti podataka, Official Gazette 42/2018, enacted by Croatian Parliament on 27 April 2018.

3 Zakon o zaštiti osobnih podataka, Official Gazette 103/03, 118/06, 41/08, 130/11, 106/12).

4 Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, Official Gazette 68/18.

5 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

When it comes to flexibilities incorporated in the GDPR, the Act introduced several flexibilities when it comes to genetic and biometric data, video surveillance and data processing for statistical purposes. For instance, the Act specifies in its Article 20 that processing of genetic data is prohibited for the purpose of risk assessment to determine the possibility of illness or other health aspects with respect to concluding and fulfilling life insurance contracts. Such a prohibition applies regardless whether the data subject gave his or her consent to such processing. However, it must be noted that such a prohibition is geographically limited to data subjects who conclude life insurance agreements in Croatia and only if the data controller is established or is providing services in Croatia.

Furthermore, with respect to biometric data, the Croatian legislator enacted the possibility of its processing by the public authorities if two conditions are met. Firstly, it must be prescribed by law, and, secondly, it must be necessary for the protection of persons, property, classified data or business secrets. However, it must be balanced that data subject's interest contrary to processing purpose shall not prevail. For example, according to article 21(2) one of such purposes explicitly prescribed by the law is fulfilling one of the obligations arising from international agreements regarding the border crossing personal identification. On the other hand, when it comes to biometric data processing conducted in the private sector, in addition to the abovementioned two conditions (for the public authorities), the legal basis has to be the explicit consent given by the data subject in accordance with the GDPR. Furthermore, the Croatian legislator explicitly allowed biometric data processing by the employers for the purpose of recording working hours and the time of the entrance and exit from the premises. However, the explicit consent of the data subject is necessary.

Furthermore, the Croatian legislator set out certain specifications (articles 25 – 32) when it comes to data processing through video surveillance. It must be noted that the Act regulates only video surveillance when such processing contains creating and storage of video recording which forms or is intended to form a part of a filing system. However, it envisions the subsidiary application of the Act only when no other more specific law is applicable. Without going into specific conditions and requirements for each situation set out by the Act, this report will as an example refer to the one prescribed by the article 30. According to that provision, processing through video surveillance can entail recording of the working space of the employees provided that employees have been informed about it by the employer before the decision of introducing such a measure has been brought. Spaces for personal hygiene, dressing rooms and leisure rooms are, however, excluded.

Finally, the Croatian legislator allowed that when the processing is conducted for the purpose of official statistics, official bodies conducting such statistics are not obliged to ensure the data subjects' rights to access, rectification, restriction of processing and the right to object in so far as those rights could probably disable or endanger the purpose of processing and when such restrictions are absolutely necessary for those purposes. Similarly,

data controllers, pursuant to article 33(3), are not obliged to inform the data subject of the data transfer if such a transfer is done to official bodies for the purpose of official statistics.

With respect to the abovementioned flexibilities introduced by the Act, it does not specify any specific powers of the Agency as the national supervisory authority besides the ones it regularly conducts, which will be further elaborated below.

Question 2

The Charter of Fundamental Rights of the European Union (hereinafter "Charter")[6] contains distinct provisions to protect the right to respect for private life and the right to data protection. Similarly, the Croatian Constitution[7] contains two separate provisions – one concerning the right to personal and family life set out in article 35 while the right to data protection is set out separately in article 37. The exact wording of the norms is the following:

> *Article 35*
>
> *Respect for and legal protection of each person's private and family life, dignity, and reputation shall be guaranteed.*
>
> *Article 37*
>
> *The safety and secrecy of personal data shall be guaranteed for everyone. Without consent from the person concerned, personal data may be collected, processed, and used only under the conditions specified by law.*
> *Protection of data and monitoring of the operations of information systems in the state shall be regulated by law.*
> *The use of personal data contrary to the express purpose of their collection shall be prohibited.*

In that respect, the Croatian Constitutional Court in its case law when determining whether there was a breach of one's constitutional right separately analyses the abovementioned

6 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

7 Ustav Republike Hrvatske, Official Gazette 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.

rights.[8] However, this differentiation did not result from distinct provisions set out by the Charter. It is present in Croatian Constitution since the amendment made in 1997.[9] With that in mind, it is hard to provide a comprehensive answer on the question whether the Charter right to data protection influenced the interpretation of national law. Furthermore, it must also be borne in mind that Croatia is the newest member state, which is still bearing the legacy of the former socialist legal tradition where national courts are primarily seen in the role of law appliers rather than lawmakers. In a system like that, it is hard to ascertain precisely what interpretive tools the judges have used.[10] According to the case law databases available to the rapporteur, up to the time of this report, there are no judgments from which can be inferred that national courts relied on the Charter. However, it is worth mentioning that in some cases parties did rely on the provisions of the Charter.[11]

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

It is quite a difficult task to give a full and comprehensive answer on the question how have data controllers interpreted and applied the principles of fair processing, purpose limitation and data minimisation for two main reasons. Firstly, the term data controller is extremely broad as it encompasses all legal and physical persons who are conducting personal data processing regardless of the sector in which they provide its services. Namely, not only do they collect various types of personal data that can be more or less sensitive, they also use it differently, for different purposes. Secondly, the principles are inherently vague and subject to interpretation, thus making it almost impossible to precisely determine its content by the data controllers and processors. This report will, thus, in answering this

8 As one of the examples of analysis of both Article 37 (data protection right) and Article 35 (private and family life) see S.B. v Županijski sud u Zagrebu, U-III-164/2013, Croatian Constitutional Court, 8 May 2014.

9 Official Gazette, 135/97, Article 5, 15 December 1997.

10 For a detailed discussion of interpretation of Croatian law in conformity with EU law, see Antonija Ivančan and Davor Petrić, "Are Croatian Courts Prepared for the Interpretive Obligation?" (2019) 44 Review of Central and East European Law 493–526.

11 See for example, M.M. v Google Hrvatska d.o.o., Municipal Court in Zagreb, Pn-3784/14, 30 November 2016.

question rely on the examples and principle analysis given by the Personal Data Protection Agency (hereinafter "the Agency") in its Annual Report[12].

As one of these examples, the Agency was dealing with was whether the collection and transfer of personal data by a non-governmental organisation to a company for the purposes of organising a referendum was to be considered lawful even without specific consent of data subjects.[13] The Agency concluded that it was, observing the principle of lawfulness and data minimisation. Namely, in order to be able to request a referendum, a petitioner (here non-governmental organisation) must prove that a certain number of people signed a petition. Since that is prescribed by the law, the Agency concluded that the legal basis set out in article 6(1)(c) or (e) applies and that the collected data is necessary for identifying people who signed the petition.

Secondly, regarding the principle of data minimisation and purpose limitation, the Agency was requested to give an official opinion on the matter whether it is lawful for the employers to send biographies to potential clients residing/established in Croatia or abroad. When answering what kind of data could lawfully be processed and transferred, the Agency relied on the principles of proportionality and data minimisation. It, thus, concluded that the data which can be included in such a transfer (without the consent of the data subject) shall be limited to information strictly relating to professional experience and/or knowledge of the employees.[14] Similarly, in another case, the Agency was requested to issue an Opinion on the question whether it is lawful for an employer, a public authority body, to send the photocopies of the ID cards of the employees to third persons. The Agency, relying on the principle of proportionality and data minimisation, enumerated which conditions must be satisfied and concluded that the sending of the photocopies would in principle be lawful. However, it stressed that the principle of purpose limitation and data minimisation must be ensured in a way that if the purpose can be achieved with a less restrictive measure, such as e.g. "checking the ID cards without making copies", such a measure shall be applied.[15]

Thirdly, another example where the Agency was dealing with the principles of fair processing, data minimisation and purpose limitation[16] was one regarding the publication of personal data pursuant to the Act on the right to access information (Zakon o pravu na

12 Godišnje izvješće o radu Agencije za zaštitu osobnih podataka za razdoblje od 1. siječnja 2018. do 31. prosinca 2018, www.sabor.hr/sites/default/files/uploads/sabor/2019-04-02/154602/IZVJESCE_AZOP_2018.pdf. All webpages referred to were visited 20 February 2020.

13 Annex to the Annual Report, Mišljenja, primjeri i preporuke Agencije za zaštitu osobnih podataka, Prilog Godišnjem izvješću o radu Agencije za zaštitu osobnih podataka za razdoblje od 1. siječnja 2018. do 31. prosinca 2018, p. 4, www.sabor.hr/sites/default/files/uploads/sabor/2019-04-02/154603/PRILOG_AZOP_2018_MISLJENJA_PRIMJERI_PREPORUKE.pdf.

14 Ibid, p. 31-34.

15 Ibid, p. 10.

16 Ibid, p. 39.

pristup informacijama).[17] Namely, pursuant to the mentioned Act, some documents concerning the financial activity of a health institution were made available online to the public. Those documents contained the personal data of identified people such as their pay check, travel expenses and education and some of the personal data subjects filed a complaint with the Agency as a National State Authority. The Agency rejected such a complaint arguing that the publication is lawful as it was made pursuant and in accordance with the limitations set out by the Act on the right to access information. It further acknowledged that the case in question deals with two constitutional rights – the right to personal data protection and the right to access to information and that a balance shall be made. It concluded that in the present case, the public interest must prevail. It concluded in such manner because all the limitations envisioned by the principle of data minimisation, purpose limitation and proportionality were ensured.

There are also examples where the Agency determined that there had been a breach of these principles. One of such examples is the one where a personal identity of the human trafficking victim, together with photographs and health data, was published online and in print.[18] The publisher pointed out that the purpose was to raise awareness of the system deficiencies and problems regarding human trafficking. The Agency concluded that pursuant to the Media Act[19] it is a valid purpose to raise public awareness. However, the same purpose could be achieved with a less invasive method, as it involves sensitive personal data that was inexcusably excessively used contrary to the principles of data minimisation and purpose limitation.

Finally, when it comes to principle analysis before the courts, according to the Agency annual report there are several cases pending before administrative courts. However, after the enactment of the GDPR there are currently no decisions issued by Croatian courts.

Question 4

According to accessible case law databases, it has not been any decision issued by the Croatian courts regarding the "consent" and "legitimate interests" as legal bases. However, there is an example present in the report by the Agency dealing with that issue when being requested for the Opinion. Namely, the question was raised whether it was lawful for an employer to send biographies of its employees to potential clients without their specific consent. The Agency, following Opinion no. 249 of the Article 29 Working Party[20], concluded that such a transfer would be lawful if the employer had a legitimate interest to

17 Zakon o pravu na pristup informacijama, Official Gazette NN 25/13, 85/15.
18 Annex to the Annual Report (2018), p. 40.
19 Zakon o medijima, Official Gazette NN 59/04, 84/11, 81/13.
20 Article 29 Working Party, 'Opinion 2/2017 on data processing at work (WP 249, 8 June 2017).

send the biographies to its potential clients. However, it pointed out that it should include only personal data which were decisive for employing the subject such as formal education, knowledge and expertise and those that are not relevant for performance of a task, such as photography or an address, shall be excluded. It further determines that when making such an assessment, a principle of proportionality must be observed in a sense that it does not include data that is not strictly necessary for its purpose.[21]

Question 5

Since entering in the European Union, together with the technological advancement, provision of information services such as Netflix and Deezer has increased. People are more and more starting the subscriptions either for free or for certain compensation. Regardless, in order to enjoy such services, when accepting terms and conditions of use, they must give their personal data as "counter-performance". So far in Croatia, there has not been a wide discussion on the validity of such a concept. However, it should be pointed out that when it comes to the provision of information society service to children, the Croatian legislator enacted a specific norm, pursuant to article 8 GDPR, which sets out 16 years old as age limit for being able to give consent.

Question 6

Even though article 22 of the GDPR (on the right not to be subject to automated decision/making, including profiling) allows Member States to introduce legislative measures to ensure this right does not apply in certain situations, the Croatian legislator has not introduced such a measure.

Question 7

The right to erasure, even though it is quite popular, has so far scarcely been used by the courts and the Personal Data Protection Agency. According to the case law databases accessible to this rapporteur, there is only one decision issued by the Municipal Court in Zagreb (first instance court) under no. Pn-3874/14.[22] A citizen M.M., relying on the recent Court of Justice of the European Union (hereinafter "CJEU") judgment in *Google Spain* initiated proceedings against Google Croatia d.o.o. (ltd.) asking for the removal from the

21 Annex to the Annual Report, 2018, p. 33.

22 M.M. v Google Hrvatska d.o.o., Municipal Court in Zagreb, Pn-3784/14, 30 November 2016.

Google search engine of several URLs containing information about him.[23] The Applicant claimed the information to be false and damaging to his professional reputation. Namely, he claims that the existence of such URLs in the Google search engine significantly impacts his ability to find a job. The Applicant previously filed an online request to Google Inc. However, the request was denied as Google Inc found the information those URLs contained of high importance to the public and interests of freedom of expression. Google Croatia d.o.o. contested its liability (passive legitimation) as it does not operate the search engine and thus cannot be considered a data controller within the meaning of Directive 95/46 EC.[24] The Court accepted that Google Croatia d.o.o. cannot be considered as data controller since it does not have any control over the use of the search engine and data and ruled in favour of Google Croatia d.o.o. The applicant filed an appeal and the case is now pending before the Regional Court in Dubrovnik (Gž – 32/2017).

Furthermore, regarding the search engines, according to data available to the rapporteur, there have not been any cases with respect to Croatian search engines that have been dealing with the right of erasure.

Finally, according to Croatian Personal Data Protection Agency's annual report for 2018 there have been several requests made by the citizens for the interpretation of the data subject's rights including the right to erasure and most of the cases are currently pending before Administrative courts.[25]

Question 8

According to the official communication between the Croatian Ministry of Public Administration and the European Commission[26], pursuant to Article 85(3) GDPR, the Croatian Ministry informed that "in relation to processing for journalistic purposes or and the purposes of academic, artistic or literary expression, the Act stipulates no exemptions or derogations from the specific chapters of the GDPR (chapters II, III, IV, V, VI, VII and IX), but instead leaves this matter to be regulated by special regulations governing those areas".[27] However, in the abovementioned letter the Ministry pointed out that "Article 14 of the Act stipulates a legal obligation of all central state administration

23 Judgment of 13 May 2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Google Spain)*, ECLI:EU:C:2014:317.

24 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L281/31.

25 Annual report of the Croatian Data Protection Agency, 2018, p. 37, www.sabor.hr/sites/default/files/uploads/sabor/2019-04-02/154602/IZVJESCE_AZOP_2018.pdf.

26 Letter of June 15th 2018, https://ec.europa.eu/info/sites/info/files/hr_notification_art_51.4_84.2_85.3_88.3_90.2_publish_0.pdf.

27 Zakon o provedbi Opće uredbe o zaštiti podataka, Official Gazette 42/2018.

authorities and other state authorities to submit to the Agency all draft proposals of laws and other regulatory proposals dealing with issues concerning the processing of personal data, for the Agency to provide professional opinions with regard to the area of personal data protection. This is to ensure a full and proper application of all the principles and provisions of the GDPR in the course of adoption of the legislation".

C Domestic Enforcement of Data Protection Law

Question 9

Article 4 of the GDPR Implementing Act sets out that the supervisory authority in the sense of article 51 of the GDPR is the Personal Data Protection Agency (Agencija za zaštitu osobnih podataka). It has been established as an independent state authority, autonomous and independent in its work. The Agency is the only and lead national supervisory authority for personal data protection in Croatia. The Agency is headed by a director, who has a deputy. The director and the deputy director of the Agency are appointed by the Croatian Parliament at the proposal of the Government of Croatia, based on the public call for candidates, launched by the central state administration authority competent for the state administration system. The director and the deputy director of the Agency are appointed for a term of four years and cannot be appointed to that office more than twice.

According to the abovementioned legislation, the Agency is entitled/obliged to perform the following tasks which can be divided in four groups:

1. Supervisory tasks

   The Agency monitors and supervises:
   - compliance and application of the GDPR Implementing Act;
   - compliance and application requests and provisions of the GDPR;
   - compliance and application of the Act on protection of physical persons with respect to processing and exchange of personal data for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
   - personal data processing for the purpose of prevention, investigation, discovery and prosecution of criminal offences or the execution of criminal sanctions, on the basis of relevant national law;
   - lawfulness of the processing, in accordance with national law and the GDPR and informs the data subject within a reasonable period of the investigation carried out or reasons why the investigation was not carried out;
   - represents Republic of Croatia before European Data Protection Board;

- cooperates with other supervisory authorities to provide mutual assistance with a view to ensure the consistency of application and enforcement of the law;
- cooperates with other guesting supervising authorities with power to conduct joint operations, including investigations and joint enforcement measures;
- acts upon the request of public authorities, with respect to assessment of lawfulness of the processing of personal data;
- acts upon the objection by the data subject;
- upon its request, it provides the data subject with the relevant information regarding the exercise of its rights granted by the Personal Data Protection Act (where appropriate it cooperates with other national supervisory authorities);
- verifies the accuracy of claims set out in the complaint lodged by the data subject and informs the data subject within a reasonable period of the progress and the outcome of the complaint, especially, if some further investigation needs to be conducted;
- issues decisions and expert opinions regarding the personal data processing, which can potentially create high risk of data subjects' rights and freedoms violations;
- publishes its opinions and decision (when publishing on web sites, the opinions and decision are anonymised and pseudonymised);
- publishes decisions (against which there is no legal remedy possible) without anonymising personal data, provided that by that decision, the Agency has determined the violation of provisions of the GDPR and/or Personal Data Protection Act with respect to minor's personal data, special categories of data, automated decision-making, profiling etc.;
- issues decisions against pronounced measures; against those decisions it is possible to start proceedings before the Administrative court (*upravni spor*);
- when the decision becomes enforceable, the Agency performs control supervision of its enforcement;
- informs relevant judicial authorities about Personal Data Protection Act violations;
- initiates and conducts proceedings against relevant persons for GDPR or Personal Data Protection Act violations;
- participates in legal proceedings conducted for enforcement of Personal Data Protection Act provisions;
- in the course of misdemeanour proceedings conducts all the measures to which the Agency is entitled to by the law. For such measures, it appoints a special representative;
- suspends the proceedings before administrative courts and passes them to the High Administrative Court of Croatia, if the Agency has reasons to doubt in the validity of the European Commission's adequacy decision or of the standard contractual clauses;

- has the power to pronounce administrative monetary sanctions and measures;
- enables the setting up of efficient mechanism for encouragement of confidential reporting on Personal Data Protection Act violations;
- follows and studies the problems regarding the processing of personal data and their impact on its protection, especially with respect to the development of new technology.

2. Advisory tasks:
   - Advises the Croatian Parliament, Government and other institutions and public authority bodies on legislative and administrative measures dealing with the processing of personal data;
   - Conducts advisory procedures on personal data processing;
   - Advises the data controller and gives opinions on every question dealing with personal data protection at its own initiative or following the request;
   - Issues opinions and approves drafts of codes of conduct;
   - Issues standard contractual clauses;
   - Authorises binding corporate rules;
   - Enforces and monitors compliance with the code of conduct;
   - Takes the necessary measures (together with appropriate safeguards) in the events of controllers or processors violating code of conduct;
   - Promotes and raises public awareness and understanding of risks, rules, and safeguards concerned their rights in relation to the processing of personal data;
   - Conducts activities of promoting awareness of individuals, controllers and processors and other target groups;
   - Continually promotes the awareness of controllers and processors, responsible for personal data processing, of their obligations arising from the Personal Data Protection Act and the GDPR;
   - Issues criteria for determining the height of the administrative costs when data subject's complaints are manifestly unfounded or excessive or are of repetitive character.
3. Corrective tasks:
   - Determines violations, issues warnings and reprimands
     - issues warnings to a controller or processor that intended processing operations are likely to infringe Personal Data Protection Act;
     - issues official reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR.
   - Has the power to order controller or processor:
     - to comply with the data subject's requests to exercise his or her rights;
     - to bring processing operations into compliance with the provisions of the GDPR and the Personal Data Protection Act (in a specified manner and within a

specified period), especially in a way to order rectification or erasure of personal data or restriction of processing pursuant to article 17 of the GDPR;
    - to communicate a personal data breach to the data subject;
    - the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed.
  - orders suspension of data flows to a recipient in a third country or to an international organisation;
  - may suspend the controller or processor from the code;
  - has the power to withdraw a certification or to order the certification body to withdraw a certification issued, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
  - imposes an administrative fine, in addition to, or instead of measures depending on the circumstances of each individual case.
4. Investigative tasks:
  - carries out investigations in the form of data protection audits;
  - imposes a temporary or definitive limitation including a ban on processing;
  - obtains access to:
    - all personal data and all information necessary for performance of its tasks;
    - any premises of the controller and the processor;
    - any data processing equipment and means;
  - where appropriate, it may:
    - make copies of available documents, record all the data and content contained in the filling systems and assemble all other relevant information;
    - seize necessary filling systems and equipment containing other relevant information and withhold it for a period necessary for making such copies;
    - confiscate filling systems or equipment when performing data protection audits;
  - if the Agency, upon performing investigative tasks, gains knowledge or finds objects suggesting commitment of a crime, it is authorised to inform the competent police station or district attorney.
5. EU and international tasks of the Agency:
  - Continually monitors data protection regulation in the country and abroad;
  - Cooperates with national supervisory authorities of the other EU Member States;
  - Cooperates in working groups and bodies, sub-groups, coordinations of the Council of European Union and of the Council of Europe;
  - Cooperates with other data protection authorities from neighbouring countries which are not EU member states;

6. Reporting tasks:
   - Draws up an annual report on its activities and transmits such a report to the Croatian Parliament. Such a report must contain all the relevant information pursuant to special law;
   - Upon the European Commission's request it submits the annual report on the GDPR Implementing Act requests through national law to the Commission and the European Data Protection Office.

Question 10

Pursuant to Article 34 of the GDPR Implementing Act, the Personal Data Protection Agency, as national supervisory authority, is given the task to conduct administrative proceedings in which it must adopt a decision whether there was a breach of the personal data protection regulation. When the Agency acts in such a capacity, there are two kinds of proceedings – one is when proceedings are initiated upon request (by anyone who claims that his rights granted by the data protection provisions have been violated) while the other is when proceedings are initiated by the Agency itself (ex officio). Regardless, the Agency when conducting such proceedings acts in a manner pursuant to General Administrative Procedure Act[28] and personal data protection laws. It is worth mentioning that after the enactment of the GDPR Implementing Act, the role of the Agency, as supervisory authority over personal data protection, has been strengthened due to the enactment of provisions on control of personal data (by an entitled person), on types of control (announced or not announced), on concrete measures which can be undertaken and on making an official report when performing the aforementioned control.

At the end of such administrative proceedings, after all the relevant facts have been determined, the Agency issues a decision (*rješenje*). The decision is issued in the form of administrative act against which no appeal can be lodged. However, the dissatisfied party can initiate proceedings before the Administrative court (*upravni spor*) where it can challenge the validity of such a decision. Those court proceedings are conducted pursuant to Croatian Act on Administrative Court Proceedings.[29]

In such proceedings the Agency performs its investigative and corrective tasks which are already mentioned above. Namely, investigative tasks are performed mainly through exercising control and performing audits over personal data processing while corrective tasks are performed when the Agency issues decisions ("rješenje") by which it issues warnings, official reprimands, orders or prohibitions to data controllers and processors.

28 Zakon o općem upravnom postupku, Official Gazette 47/09.

29 Zakon o upravnim sporovima, Official Gazette 20/10, 143/12, 152/14, 94/16, 29/17.

When issuing a measure The Agency determines takes into account the level of seriousness of personal data protection infringement. The issued measures may be of temporary or permanent nature which is also determined on a case-by-case basis.

Finally, after the enactment of the GDPR Implementing Act, pursuant to article 44 of that Act and article 83 of the GDPR, the Agency is also entitled to impose pecuniary administrative fines. However, it must be mentioned that when it issues such fines, the decision is brought in the form of "*odluka*" instead of "*rješenje*". Against such a decision, there is also no possibility to lodge an appeal, but the dissatisfied party may also initiate administrative court proceedings before the competent Administrative court pursuant to the Act on Administrative Court Proceedings. Nevertheless, the Agency, pursuant to article 47 of the GDPR Implementing Act, cannot issue administrative fines in proceedings against public authority bodies. When it issues such administrative fines, the Agency publishes the decision on its web page without anonymising personal data of the entity that made an infringement.

Question 11

According to the annual report of the Agency, following the GDPR entering into force on May 25th 2018, the number of received complaints has grown. Namely such a conclusion is inferred from the fact that the number of complaints received by the Agency in 2018 (356) outreaches the number of complaints received in 2017 (139) by almost 260% percent. The complaints have been received in various sectors (banking and finance, marketing, health organisation etc.), which will be further elaborated in the text below.

One of the sectors in which the Agency received a large number of requests for opinions as well as complaints was the public sector. Such a number was expected considering that there is a vast number of personal data controllers and processors present within. In that respect, the Agency, if it found that processing was contrary to data protection provisions, for instance, ordered employers to cease processing personal data for which there was no lawful basis. The practical examples are the following:

- the Agency prohibited video recording of working premises which shall not be subject to such a recording;
- the Agency prohibited collecting and processing of personal data when it found that it exceeded the amount necessary for the purposes for which they were processed;
- the Agency prohibited collecting and further processing of personal data when it was determined that they were not collected for the precisely defined purpose.

Moreover, a large number of complaints was received in the finance sector, especially considering the question whether making a copy of an ID card (pursuant to the Act on

Anti-Money Laundering Terrorism Financing)[30] was in accordance with the data protection laws. Other complaints were mostly received by the banking and other credit institutions clients with respect to the due diligence procedure when entering into a business relationship or making a transaction. In that respect, the Agency, not only was solving the received complaints, but also conducted preventive measures in order to raise awareness of the credit institutions and to draw attention to possible incompliances when collecting and further processing personal data of their clients. To be precise, such measures were primarily aimed at questionnaires the institutions were giving to their clients when performing the due diligence procedure.

Further on, in the health organisation sector, the Agency was dealing mostly with the complaints whether publication (in the public media) of their diagnosis and personal data is compliant with the data protection regulation. Moreover, the Agency determined that in this sector, some of the employers were unlawfully transferring medical data and documentation to third parties. In such cases, the Agency prohibited further processing and transferring and ordered the employers to conduct necessary safety measures.

Finally, in the telecommunications sector, individuals raised complaints claiming identity theft. Many complaints concerned the conclusion of a contract without authorisation, using the individual's personal data. The Agency found most of the complaints founded and as they also indicated that a crime had taken place, the Agency properly notified the police and the district attorney. Identity theft complaints were also present in the online environment. One of these examples involved the use of Facebook pages in order to collect and further process personal data. The violators have been organising a false prize contest where the person who applied gave his/her personal data.

Question 12

The Croatian legal system has historically awarded damages for intangible harm. Namely pursuant to Article 19 of the Croatian Civil Obligations Act (*Zakon o obveznim odnosima*)[31] any natural person or legal entity is entitled to the protection of its personality rights. According to the second paragraph of the mentioned article, under personality rights, among other rights, the right to privacy of personal and family life is also understood. Furthermore, according to article 1100 of the mentioned Act in the event of violation of personality rights, the court shall, where it finds that this is justified by the seriousness of the violation and circumstances, award a just pecuniary compensation, irrespective of the compensation for material damage and in the absence of the latter. In deciding on the

30 Zakon o sprječavanju pranja novca i financiranju terorizma, Official Gazette NN 108/17, 39/19.
31 Zakon o obveznim odnosima, Official Gazette 35/05, 41/08, 125/11, 78/15, 29/18.

amount of just pecuniary compensation, the court shall take into account the degree and duration of the physical and mental pain and fear caused by the violation, the objective of this compensation, and the fact that it should not favour the aspirations that are not compatible with its nature and social purpose.

Moreover, the practice of the Croatian courts, when dealing with the matter of intangible harm, created criteria for calculating the damages ("just pecuniary compensation"). The Croatian Supreme Court in 2002 issued a document titled "Guidance criteria for determining the amount of just pecuniary compensation".[32]

Question 13

Pursuant to article 502a of the Civil Procedure Act,[33] a mechanism of collective redress was already introduced. In that respect the GDPR Implementing Act has not introduced anything new. For the time being, there have been no such proceedings initiated before Croatian courts.

Question 14

The Agency has been cooperating with other public authorities, including the ombudsman. Namely, such a cooperation is visible on the Agency's webpage where it encourages data subject's to consult the ombudsman when they believe their rights have been violated.[34]

D Data Processing for National Security Purposes

Question 15

The term 'national security' is not defined in the Croatian law nor by administrative practice. However, there are certain acts and bylaws that have to be mentioned when it comes to 'national security' especially in the context of data retention, as they are regulating powers and authorities. Regarding the acts primarily relevant is the Act on security

32 Su-1331-VI/02 and 1372-11/02, Croatian Supreme Court, Zagreb, 29 November 2002.

33 Zakon o parničnom postupku, Official Gazette 4/77, 36/77, 6/80, 36/80, 43/82, 69/82, 58/84, 74/87, 57/89, 20/90, 27/90, 35/91, i NN 53/91, 91/92, 58/93, 112/99, 88/01, 117/03, 88/05, 02/07, 84/08, 96/08, 123/08, 57/11, 148/11, 25/13, 89/14.

34 https://azop.hr/obavijesti/detaljnije/pucki-pravobranitelj.

intelligence systems[35] and the Act on homeland security.[36] Furthermore, with respect to bylaws this report will point out the National Security Strategy[37] adopted by the Parliament and the Regulation on obligations arising from national security of physical and legal persons in telecommunications sector.[38] Those documents provide a legal framework for the operations taken by the national authorities. However, for writing this report there was no data on the actual practice.

Furthermore, when it comes to the question of recognising the Charter, as was briefly mentioned above, Croatian courts, due to the traditionalist civil law culture, have a tendency not to explicitly rely on the Charter when issuing a decision. Therefore, there is no evidence (accessible for this report) that may indicate whether national authorities have accepted the application of the Charter to data retention for national security purposes.

35 Zakon o sigurnosno-obavještajnom sustavu, Official Gazette 79/06, 105/06.

36 Zakon o sustavu domovinske sigurnosti, Official Gazette 108/17.

37 Strategija nacionalne sigurnosti Republike Hrvatske, Official Gazette 73/17.

38 Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama, Official Gazette 64/08, 76/13.

Cyprus

Stéphanie Laulhé Shaelou and Katerina Kalaitzaki[*]

A Setting the Scene

Question 1

The House of Representatives in Cyprus adopted the national law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data (Law 125(I)/2018), on 31 July 2018. The law was adopted for the effective implementation of certain provisions of the General Data Protection Regulation (hereinafter "GDPR"), which applies as of 25 May 2018.[1] Upon entry into force of the provisions of law 125(I)/2018, the Processing of Personal Data (Protection of Individuals) Law of 2001 (Law 138(I)/2001) was repealed while Acts issued by the Commissioner under the provisions of the Processing of Personal Data (Protection of Individuals) Law, which is repealed, will continue to be valid until their expiration or replacement.

Most of the notable flexibilities incorporated in the GDPR have been implemented in law 125(I)/2018. For instance, article 6(1)(c) GDPR which states that 'processing is necessary for compliance with a legal obligation to which the controller is subject' has been implemented in particular in sections 5-7 of the relevant law under the title 'Part II: Lawfulness of Certain Processing Operations'. Section 5 permits the lawful processing of personal data when it is carried out by the Courts acting in their judicial capacity and by the House of Representatives within its powers. Moreover, section 6 permits the lawful processing of special categories of data when 'it is carried out for the purpose of publishing or issuing a decision of any court or when it is necessary for the purpose of delivering justice'. Lastly, within the framework of compliance with a legal obligation, section 7 permits the processing of personal data 'on the basis of a Decision of the Council of Ministers to a public authority or body for the performance of a task carried out in the

* Stéphanie Laulhé Shaelou: Professor of European Law and Reform and Head, School of Law, University of Central Lancashire, Cyprus. Katerina Kalaitzaki: Post-Doctoral Fellow (at the time of submission), School of Law, University of Central Lancashire, Cyprus. This report is up to date as of 30 August 2019. All webpages referred to were visited on 30 August 2019.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

public interest or in the exercise of official authority'. Beyond the processing necessary for the compliance with a legal obligation, further categories where processing of data is allowed were added in the law including the offering of information society services to a child, while the processing of genetic and biometric data for purposes of health and life insurance is prohibited.

Part IX of law 125(I)/2018 entitled 'Processing of personal data in specific situations', lays down a list of situations where the processing of personal data is allowed in exceptional cases corresponding to articles 86-90 GDPR. Article 86 allowing the disclosure of personal data in official documents held by a public authority or body for the performance of a task carried out in the public interest was implemented under section 30 of the law. Regarding article 87 GDPR, the Cypriot legislator partly determined the specific conditions for the processing of a national identification number under section 10(2) of the law stating that in cases where the combination of filing systems by public authorities relates to special categories of personal data or to personal data relating to criminal convictions and offences or is to be carried out with the use of the identity card number or any other identifier of general application, it is required to undertake a data protection impact assessment and a prior consultation with the Commissioner.

Article 89 GDPR concerning the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes was transposed under section 29 law 125(I)/2018. Section 29(1) states that 'the processing of personal data or special categories of personal data or personal data relating to criminal convictions and offenses, which is carried out for journalistic or academic purposes or for purposes of artistic or literary expression, is permitted, provided that those purposes are proportionate to the aim pursued and respect the essence of the rights as set out in the EU Charter and the ECHR'. Lastly, section 31 states that 'the processing which is carried out by a controller or a processor for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be used for taking a decision which produces legal effects concerning the data subject or similarly significantly affects him or her'. Article 88 GDPR, concerning the processing in the context of employment was not implemented in the law to provide for more specific rules to ensure the protection for the rights and freedoms of employees' personal data, although according to the Regulation this can also be done by collective agreements. Therefore, this omission of the House of Representatives does not seem to create a gap for the protection of employees.

Beyond the GDPR, Member States had to transpose the Data Protection Law Enforcement Directive (hereinafter "LED") into their national law by 6 May 2018.[2] The

2 Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

Directive protects citizens' fundamental right to data protection whenever criminal law enforcement authorities for law enforcement purposes use personal data. EU rules ensure that the personal data of victims, witnesses, and suspects of crime are duly protected. The introduction of similar data protection standards facilitates the exchange of personal data for cross-border cooperation in the fight against crime and terrorism.[3] As Cyprus failed to transpose EU rules into national legislation, the Commission sent a letter of formal notice to the relevant authorities in July 2018. The Commission had sent a reasoned opinion to Cyprus for failing to implement the LED on 24 January 2019, which granted Cyprus two months to respond and take the relevant action; otherwise, the case could be referred to the Court of Justice of the EU (hereinafter "CJEU").[4] The Directive was transposed in March 2019 under Law 44(I)/2019.[5]

Question 2

Article 7 Charter of Fundamental Rights of the European Union (hereinafter "Charter") enshrines the right to respect for private and family life while article 8 the protection of personal data. The Constitution of Cyprus includes a long list of fundamental rights and liberties under Part 2, inspired by the European Convention on Human Rights (hereinafter "ECHR"), and an express reference to the right of a person to have respect for his private and family life is made under article 15 as well as to a further right to privacy of correspondence in article 17. Subject to the analysis of articles 15 and 17 of the Constitution provided in Part D below, no express reference to the protection of personal data is made within the Constitution itself. Moreover, law 125(I)/2018 does not make any reference to article 8 or to any other specific right of the Charter. The only express reference made to the Charter is a very generic one under section 29(1) of the said law, of relevance to Question 8 below. Contrary to the main body of legislation, the Commissioner has made extensive references to articles 7 and 8 Charter in her decisions when setting out the relevant legal framework of a case, in conjunction with article 8 ECHR and article 15 of the Constitution of Cyprus.[6]

---

criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L119/89.

3 https://in-cyprus.com/european-commission-to-seek-legal-action-against-cyprus-over-nine-infringements/.

4 https://europa.eu/rapid/press-release_MEMO-19-462_en.htm.

5 Law of 2019 (44(I)/2019) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (in Greek).

6 Decision No. 135/2018, 9 January 2019, para. 2.8., www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/2566119727D4B95CC22583A2003987DF/$file/complaint%20135-2018-efimerida%20politis-apofasi.pdf?openelement; Decision No. 192/2018, 12 April 2019, para. 2.5. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

In the run-up to the entry into force of the GDPR, data controllers in Cyprus have benefited from clear guidelines, information sessions and trainings, pertaining in particular to the 'general obligations' they ought to follow and apply as per article 5 GDPR. Such general obligations are issued by the Data Protection Commissioner in Cyprus and pertain inter alia to fair processing, purpose limitation and data minimisation.[7] Other general obligations relate to articles 13 and 14 GDPR.[8] General obligations have also been issued with respect to the role of accountants, auditors and lawyers acting as data processors.[9] Overall it can be said that data controllers (as well as data processors) in Cyprus have interpreted and applied such principles in line with requirements under the GDPR. It could be said that data controllers in the private sector as well as some semi-governmental organisations have perhaps been quicker and more efficient in applying GDPR requirements by putting together adequate policies and implementing them, even if violations occur. A circular was published by the State Service of Public Administration and Personnel on the management of archives and documents containing personal data in public services, dated 24 May 2018. Since the entry into force of the GDPR however, various Ministries and State services, including under the Ministry of Health, Education or the Ministries themselves, public bodies such as a hospital or a university, as well as local authorities have been issued a warning or fined for non-compliance with the GDPR, its principles, its safety measures or for lack of consent.

The Data Protection Commissioner also has the power to issue opinions to the national parliament, the government or to other institutions and bodies and/or the public, in accordance with article 58(3)(b) GDPR, which she has already used to issue three such opinions of much relevance to all economic sectors in Cyprus.[10] Such opinions are based on the principles set out in article 5 GDPR, including of fair processing, purpose limitation

BACBDB52BA83F8DEC22583F2001E4EE2/$file/%CE%91%CE%9D%CE%9F%CE%9D.%20%CE%91%CE%A0%CE%9F%CE%A6%CE%91%CE%A3%CE%97%20Breikot.pdf?openelement (in Greek).

7 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2a_gr/page2a_gr?opendocument (in Greek).

8 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/39B375E9A0126F47C22582F9002BFE2B?OpenDocument (in Greek).

9 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/341ABF6C91574B17C225830B001F5543?OpenDocument (in Greek).

10 Opinion 1/2018 addressed to all trade unions on salaries; Opinion 2/2018 on video surveillance at the workplace and the use of biometric systems; Opinion 3/2018 on access to email accounts of employees and former employees (in Greek).

and/or data minimisation, thereby reinforcing their importance.[11] Such opinions also refer to existing decisions of the Commissioner in the field, giving concrete examples and precedents to addressees of the opinions. Such opinions are complemented by sectoral circulars such as in the area of health or insurance. Reference is regularly made to EDPB Guidelines and/or to Article 29 Working Party in such instruments.

Directives issued by the Commissioner in the pre-GDPR era are still valid until provided otherwise. Recent decisions of the Commissioner are now based on the GDPR regime, using the above principles, legal bases under the GDPR as well as the implementing law. Notable post-GDPR decisions against data controllers were taken on the basis of the principle of data minimisation,[12] legitimate interest and/or lack of consent.[13]

However, the pre-GDPR regime still provides most of the ground for interpretation by the domestic courts rather than the newly established GDPR regime. The few court decisions of relevance, recently issued by the Administrative Court, relates to decisions of the Data Protection Commissioner taken under the pre-GDPR regime, which were challenged before the court. Recent appeal cases heard by the Supreme Court of Cyprus also refer to pre-GDPR decisions which have been challenged and then appealed.[14] The first recourses of post-GDPR decisions appear to be currently pending.[15]

Question 4

In view of the above limitations, it cannot really be said that the legal bases of consent and legitimate interests under the GDPR regime have yet been explored or interpreted by national courts in Cyprus, even though the first such recourse is pending.[16] Such concepts have however been interpreted by the courts under the pre-GDPR regime and/or in other contexts than data protection. With respect to legitimate interest, it should be noted that this notion forms a cornerstone of constitutional rights in Cyprus.[17]

---

11 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3f_gr/page3f_gr?opendocument (in Greek).

12 See Decision No. 192/2018, 12 April 2019, against a company part of a media group (Nikodea Media group); Decision No. 135/2018, 9 January 2019, against newspaper Politis (in Greek).

13 See Decision No. 232/2018, 12 April 2019, against Sigma Live Ltd, a media group, in violation of art. 6(1)(a) GDPR; Decision No. 135/2018, 9 January 2019, against newspaper Politis partly based on art. 6(1)(f) GDPR (in Greek).

14 Such as Appeal 32/2013, *Republic of Cyprus through Commissioner on Data Protection v Dias Publishing House Ltd*, judgment issued on 1 March 2019 (in Greek) on the protection of sensitive data and the right to family life.

15 Decision No. 135/2018, 9 January 2019, recourse before the Administrative Court pending.

16 Decision No. 135/2018, currently being challenged before the Administrative Court, was based on a breach of the principle of data minimisation, of legitimate interest and for lack of consent, under arts 5 and 6 GDPR.

17 A. Emilianides, *Constitutional Law,* Supplement, Wolters Kluwer, 2019, p. 225.

Question 5

To date, there does not seem to have been a meaningful debate or a decision at national level regarding the validity of personal data as 'counter-performance' for the provision of digital content. The Data Protection Officer has however provided clear and precise guidelines on direct marketing (pre-GDPR) as well as cookies, referencing Article 29 Data Protection Working Party, updated in 2019 but referring mainly to pre-GDPR instruments.[18]

Question 6

Processing is defined in the main law as it is in the GDPR, referring to automated means or not, but there is no reference to profiling. Law 44(I)/2019 which implements the LED transposes almost verbatim article 11(1) LED on automated individual decision-making. Section 13(1) of the law provides that 'a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited unless authorised by Union or national law to which the controller is subject'. That is provided appropriate 'safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller, are provided in the law'. Article 11(2) and (3) LED is also reproduced, with reference to safeguards for the 'data subject's rights and freedoms and legitimate interests' and discrimination.

General measures to safeguard the rights, freedoms and legitimate interests of data subjects, deriving from the GDPR, are incorporated into Part II of the main law. Section 5 nevertheless starts by providing that the processing of personal data by the Courts and the House of Representatives is permitted and lawful 'notwithstanding article 6(1)(e) GDPR', thereby suggesting that no proportionality test is needed to justify the processing of personal data by these data controllers acting within their powers. With respect to the publishing and issuing of decisions by the Courts, section 6 provides that the processing of sensitive personal data covered by article 9 GDPR is permitted and lawful. It would seem as though the Courts were exempted from the restrictive scope of the law. Nevertheless, the Supreme Court, as an independent organ of the State, issued a circular containing directives on the publication of decisions in the post-GDPR regime.[19] The circular promotes the protection of the right to privacy and family life, as may be limited through proportionality, and applies the principle of data minimisation and anonymisation

18 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/71B32C48C08B5AC1C22582780040F80E?OpenDocument (in Greek).

19 www.supremecourt.gov.cy/Judicial/sc.nsf/All/B450E5061E647886C225837C00309575?OpenDocument published on 19 June 2018 (in Greek).

to personal data as may be controlled or processed by the courts, including sensitive data as listed in the circular. The circular also provides for the conditions of publication of decisions through dedicated online platforms of Cypriot law, which prompted a public debate around the way the Supreme Court applied the GDPR.

Section 7 law 125(I)/2018 provides that the processing on the basis of a decision of the Council of Ministers must be 'performed lawfully and fairly, in a clear, precise and transparent manner in relation to the data subject, in accordance with the provisions of article 5(1)(a) and article 6(1) GDPR'. Sections 8 and 9 include specific references to consent, either of a child or 'the holder of parental responsibility over the child' for the offering of information society services to a child, or the separate consent of the data subject in case of further processing, without prejudice to the principle of purpose limitation. Under section 10, the combination of filing systems by public authorities or bodies is only permitted for reasons of public interest and subject to article 6(1)(c) or (e) or article 9(2)(g), (h) or (i) GDPR.

Question 7

In its 2017 annual report, the Data Protection Commissioner notes that the number of complaints regarding direct marketing messages or spam, leading to requests to erase personal data, were down compared to 2016 (below 150). This was probably due to the fact that the senders put in place consumer systems for erasure.[20] With respect to violations of the pre-GDPR legal regime however, the report observes that quite a few companies do not take sufficiently seriously the right to object of their consumers and that they do not have designated procedures for the efficient erasure of all numbers of consumers who do not wish to receive such messages (including in case of change of marketing company by the sender).[21] On average there seems to be a growing number of administrative decisions on the right to erasure in various economic sectors (insurance in particular), including against search engines, websites or social media platforms in Cyprus.[22] Since 2018, the number of such complaints brought before the Data Protection Commissioner appears to be on the rise. Court decisions in the field remain scarce, which could indicate that administrative decisions ordering erasure of personal data are not necessarily appealed by

20 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/64DE4B83284311F7C225836700400096/$file/Ετήσια%20Έκθεση%202017.pdf (in Greek), p. 30.

21 ibid, p. 53.

22 Decision No. 5/2016, 13 October 2016 against Facebook www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/4D64324AD8260202C2258258004124F7?OpenDocument (in Greek). See also the Decision issued on 28 March 2019 against the website Skroutz.com.cy. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/BACBDB52BA83F8DEC22583F2001E4EE2?OpenDocument (in Greek).

data controllers, perhaps in an effort of compliance. As administrative decisions however grow more complex, judicial recourses against them are expected.

Question 8

As developed in Part A above, Part IX of law 125(I)/2018 entitled 'Processing of personal data in specific situations', lays down a list of situations where the processing of personal data is allowed in exceptional cases corresponding to articles 86-90 GDPR. The duty to balance the right to the protection of personal data with the right to freedom of expression and information enshrined in article 85 GDPR is reflected in section 29(1) law 125(I)/2018. Section 29(2) also provides that the provisions of articles 14 and 15 GDPR 'shall apply to the extent that they do not impair the right to freedom of expression and information and journalistic secrecy'. As such it can be said that Cyprus has exercised its right to legislate under article 85(2) GDPR.

This does not appear to have been interpreted or applied formally to date. With respect to the pre-GDPR regime, it is worth mentioning a recent unanimous decision of the Supreme Court on appeal of a Decision of the Data Protection Commissioner, initially challenged at first instance, regarding the publication of an article in Simerini disclosing sensitive data of a child, in violation of the principle of proportionality and of privacy and family life.[23] The Supreme Court allowed the appeal on the ground that there is no automatic right of journalistic retransmission of the subject-matter of a court case. This will depend on the result of a balancing exercise to be conducted by the journalists. In the present case, there was a violation of the principle of proportionality and of privacy and right to family life.

C Domestic Enforcement of Data Protection Law

Question 9

The competent National Supervisory Authority in Cyprus is the Commissioner of Personal Data Protection, which is an independent public authority responsible for monitoring the implantation of the GDPR and other laws aiming at the protection of individuals with regards to the processing of personal data. The Commissioner performs the duties and exercises the powers assigned by the GDPR or any other relevant law in complete

23 Appeal 32/2013, *Republic of Cyprus through Commissioner on Data Protection v Dias Publishing House Ltd*, judgment issued on 1 March 2019 (in Greek).

independence and represents the Republic in the relevant bodies and committees of the EU, the Council of Europe, and other International Organisations.[24] The Commissioner is appointed in accordance with section 19 of the national law, which implements the provisions of article 51 GDPR, by the Council of Ministers upon the recommendation of the Minister of Justice and Public Order.

The duties and powers of the Commissioner are enlisted under section 23 of the law, including the power to authorise any officer of her Office, who holds a position of authority, to exercise on her behalf such duties and powers,[25] while she has no competence to supervise processing operations carried out by the courts of the Republic.[26] More importantly, the additional duties of the Commissioner are enshrined in section 24, which include the transparency duties of the Office and the procedure of handling/examining a complaint that is discussed in detail later in this Report. Section 25 sets out the additional powers of the Commissioner including the investigative powers of the Commissioner in accessing/collecting information and data,[27] the corrective powers granted to the Commissioner (discussed in more detail later in the Report),[28] as well as the authorisation and advisory powers.[29] Lastly, the Commissioner participates in the European Data Protection Board, which is composed of all Supervisory Authorities of EU Member States and the European Data Protection Supervisor, as well as by the European Commission.[30]

Question 10

The Cypriot law states under section 24(b) that subject to the provisions of article 57 GDPR, the Commissioner shall examine the complaints lodged and 'where possible depending on the nature and type of the complaint, inform the complainant in writing of the progress and outcome of the submission within 30 days'. The Commissioner shall therefore investigate the subject of each complaint as appropriate and the degree to which each complaint is dealt with is at her discretion in accordance with article 57(1)(f) GDPR. If the complaint is deemed unfounded or does not fall within the competence of the Commissioner, she shall inform the complainant in writing within 30 days of the filing of the complaint. Consequently, complaints which are vague, unfounded or excessive, particularly due to their recurring nature, or if they are anonymous and/or do not contain

24 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument.
25 s.23(2) law 125(I)/2018.
26 s.23(4).
27 s.25(a)-25(d) law 125(I)/2018.
28 s.25(e)-25(f).
29 s.25(g)-25(i).
30 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument.

the necessary details, may not be examined.[31] In such case the complainant shall be duly informed. Section 29(d) indicates that the Commissioner 'may not investigate a complaint or discontinue its investigation for reasons of public interest and shall notify to the data subject, within a reasonable period, the reasons for not investigating or for terminating the investigation of the complaint'. It thus seems that the Cypriot legislator followed the approach of the GDPR for complaint-handing, although it is not yet clear whether the public interest ground under paragraph (d) could be used to allow the Commissioner to reject minor claims to pursue the legitimate aim of achieving more effective and efficient use of resources, effective judicial protection or even sound budgetary policies.

Question 11

The national law has dedicated Part X to administrative fines, offences and sanctions. Section 32 indicates that the Commissioner shall impose administrative fines in accordance with article 83 GDPR. Where the administrative fine remains unpaid it shall be collected as a civil debt due to the Republic.[32] An administrative fine imposed to a public authority which relates to non-profitable activities shall not exceed 200,000 euro. Regarding the offences committed under Section 33(1) by the processors, controllers, certification bodies, public authorities or third persons, the sanctions vary depending on the seriousness and/or type of the offense. The most serious sanction for specific offences amounts to imprisonment of maximum 5 years and/or to a fine not exceeding 50,000 euro and for the least serious offences the convicted person shall be subject to imprisonment of a maximum of 1 year and/or to a fine not exceeding 10,000 euro. There is also a category of offences convicted with a maximum of 3 years and/or to a fine not exceeding 30,000 euro.[33] The imposition of administrative fines is the sanction mostly used by the NSA in Cyprus. For instance, the Commissioner has recently imposed a financial penalty of 10,000 euro to a newspaper for unlawful disclosure of names and pictures of two police investigators in a publication which allegedly involved inconvenience, unnecessary and unlawful detention of a citizen. The Commissioner considered that the aim could be achieved by referring only to the initials of their name and/or their faces being blurred and/or publishing photographs drawn from a distant distance so that it was impossible to identify the persons, and these actions would not bring any change in the nature of the case.[34]

31 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_gr/page1i_gr?opendocument.

32 s.32(2) law 125(I)/2018.

33 s.33(2) law 125(I)/2018.

34 Decision No. 135/2018, 9 January 2019, para. 5.3., www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/2566119727D4B95CC22583A2003987DF/$file/complaint%20135-2018-efimerida%20politis-apofasi.pdf?openelement (in Greek).

In addition to the corrective powers provided for in article 58(2) GDPR, the Cypriot law adopted further corrective powers under section 25(e). In particular, the Commissioner has the power to require the Cyprus Organization for the Promotion of Quality to revoke the accreditation of a certification body, when she ascertains that the requirements for the certification are not met or where actions taken by the certification body violate the provisions of the GDPR or the relevant national law. According to section 49 law 44(I)/2019 implementing LED, the decision issued by the Commissioner, including the decisions imposing a sanction, can be challenged before the Administrative Courts in accordance with article 146 of the Constitution, while an appeal of the Administrative Court's decision can be made before the Supreme Court.[35]

In particular, in the recent case of *Dias Publishing House*, the Commissioner had imposed an administrative fine on a local newspaper for disclosing a child's name and his health problem. The fine was challenged before the civil courts in accordance with article 146 of the Constitution of Cyprus and the Supreme Court acting in its capacity as an administrative Court (now Administrative Court) had annulled it. However, the Supreme Court's ruling on the 1st of March 2019, reversed the previous decision by rejecting the newspaper's claims and confirming the Commissioner's fine.[36]

Question 12

As discussed above, the Commissioner may impose corrective measures (including fines) to controllers or processors, when they are in breach of the data protection legislation but cannot grant compensation to affected data subjects. Contrary to article 82 GDPR, no reference is made under national law that data subjects should be compensated for damages suffered for tangible and intangible harm. Specifically, any person who has suffered material or non-material damage as a result of an infringement of the GDPR, by the controller or the processor, has the right to seek compensation before a Civil Court in accordance with the Civil Offences Law Cap. 148. Under section 3 of the Civil Offences Law, any person who suffered any damage by reason of a civil wrong (e.g. negligence, breach of statutory duties and regulations) shall be entitled to seek from the person committing or liable for such civil wrong the remedies which the Court has the power to grant.

35 Appeal 32/2013, *Republic of Cyprus through Commissioner on Data Protection v Dias Publishing House Ltd.*
36 Ibid.

Question 13

Law 125(I)/2018 does not make any reference to the representation of data subjects. On the contrary, a 'representative' is defined in the law as a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to article 27 GDPR, represents the controller or processor with regard to their respective obligations. On the other hand, law 44(I)/2019 implementing LED, includes the representation of data subjects under section 51, stating that 'the data subject shall have the right to mandate a not-for-profit body, organisation or association which has been duly constituted in accordance with the relevant national legislation, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data, to lodge the complaint referred to in section 48 and to exercise the rights referred to in sections 49 and 50 on his behalf'. It is in fact the direct implementation of article 55 LED into national law. As a result, based on section 51, the representative of the data subject shall have the right to lodge a complaint before the Commissioner, the right to an effective judicial remedy against the Commissioner and against the controller or processor.[37] The same rights that the representative of the data subject would have been entitled to if the Regulation was implemented in law 125(I)/2018.

The omission of implementing article 80 GDPR into the relevant national law seems to have slightly affected the data protection system in two aspects; (1) the fact that the right to receive compensation referred to in article 82 cannot be exercised by the representative of the data subject, which does not create any complexities since a claim for compensation can only be raised before the Civil Courts and (2) that the representative cannot act independently of a data subject's mandate to lodge a complaint with the supervisory authority as provided under article 80(2). As a result, the combination of laws 44(I)/2019 and 128(I)/2018 currently allow a complaint to be lodged firstly by the person whose data are being processed (the data subject) and secondly by a non-profit body, organisation or association as referred to in section 51 law 44(I)/2019. The information and power asymmetries created between the data controllers/processors and data subjects are thus mitigated by providing the possibility of representative actions in national law.

Question 14

During the recent years in Cyprus not many incidents have been recorded of regulators intervening in data processing related complaints. In fact, the Cypriot Ombudsman

37 s.48-50 law 44(I)/2019.

(Commissioner for Administration and Protection of Human Rights) seems to intervene only when indispensable and only in cases which involve serious human rights infringements beyond the protection of personal data. For instance, following a complaint about an excessive number of cameras used in a medical institution where a person in custody was hospitalised, the Commissioner asked the Prison Department to set criteria for the number of cameras to be placed in areas declared as cells in accordance with the Prison Law.[38] A uniform practice had to be followed on the basis of the severity of each case and the principles of proportionality, transparency and accountability. After the Prison Department informed the Commissioner of the criteria it adopted, an Officer was authorised to carry out an inspection in the site in order to determine whether the cameras in that room fulfilled the criteria set by the Prison Department itself.[39] The inspection found that a limited number of cameras did not meet the pre-determined criteria and a letter was sent to the Prisons Department to remove them in order to comply with the data protection guidelines. At that point, the Cypriot Ombudsman intervened with recommendations addressed to the Prison Department to remove the cameras and comply with the letter of the Commissioner for Personal Data.[40]

Another example is when the jurisdiction of the claims lodged is not clear and the different authorities of the government need to cooperate to guide the applicants and refer the claims to the competent office. For example, a wave of complaints was recently lodged concerning mobile phone bills that did not fall within the jurisdiction of the Commissioner, since the Commissioner is considering complaints about unsolicited advertising spam but is not empowered to charge for complaints. As a result, the Office of the Commissioner for the protection of personal data informed the applicants that they should refer the matter to the Electronic Communications and Mail Regulatory Commissioner (ERIET).[41] In addition, the Commissioner indicated that if the applicants' consent for activation of a subscription service has been diverted through misleading advertising, they can refer the matter to the Competition and Consumer Protection Office of the Ministry of Trade and Tourism.[42]

38 Office of the Commissioner for Personal Data Protection, Annual Report 2017 (Greek), p. 122 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/64DE4B83284311F7C225836700400096/$file/%CE%95%CF%84%CE%AE%CF%83%CE%B9%CE%B1%20%CE%88%CE%BA%CE%B8%CE%B5%CF%83%CE%B7%202017.pdf.

39 Ibid.

40 Ibid, p. 121.

41 Ibid, p. 56.

42 Ibid, p. 56.

D Data Processing for National Security Purposes

Question 15

In Cyprus, there appears to be no express definition of the notion of national security which would differ from the understanding at the European level of the area of national security as activities carried out by the State itself or State authorities, traditionally intertwined with the areas of public security, defence and the fighting of crime provided a vital national interest security is at stake. The Cyprus Constitution[43] provides that national security can restrict some of the fundamental freedoms protected under the Constitution, such as the right to privacy, through a proportionality test. Article 15 of the Constitution in particular provides that '[e]very person has the right to respect for his private and family life' (paragraph 1) and that '[t]here shall be no interference with the exercise of this right except such as is in accordance with the law and is necessary only **in the interests of the security of the Republic** or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the rights and liberties guaranteed by this Constitution to any person' (paragraph 2).[44] The national courts interpreted the scope of article 15 of the Constitution in landmark case law.[45] There was an amendment of article 15 of the Constitution through the Ninth Amendment of the Constitution Law 69(I)/2016 which provides that the right may also be restricted for the protection of transparency and for measures against corruption in public life.[46] Article 15 of the Constitution, as amended, has been used as a legal basis to find national legislation unconstitutional as far as transparency and corruption in public life are concerned.[47]

Also of relevance to privacy is article 17 of the Constitution which provides that '[e]very person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law' (paragraph 1). This is followed by paragraph 2 which provides that '[t]here shall be no interference with the exercise of this right, unless such interference is permitted in accordance with the law, in the following cases: A. Of convicted or unconvicted prisoners; B. Following a court order issued pursuant to the provisions of the law, upon an application by the Attorney-General of the Republic, and interference shall constitute a measure which is necessary in a democratic society only **in the interests of the security of the Republic**

43 Constitution of the Republic of Cyprus, 1960. For an unofficial English translation, see: www.constituteproject.org/constitution/Cyprus_2013.pdf?lang=en.

44 Emphasis added.

45 *President of the Republic v. House of Representatives* [2000] 3 CLR 238 (in Greek).

46 See Emilianides, p. 181.

47 App. 11-12, 14-16/2016, *President of the Republic v. House of Representatives*, judgment of 16 March 2017 (in Greek).

or for the prevention, investigation or prosecution of the following serious criminal offences: […].[48] C. Following a court order issued in accordance with the provisions of the law, for the investigation or prosecution of a serious criminal offence in respect of which, in case of conviction, a sentence of imprisonment of five years or more is provided and the interference concerns access to relevant electronic communication data of movement and position and to relevant data which are necessary for the identification of the subscriber or and the user' (paragraph 2). Again national courts have interpreted this constitutional provision in landmark case law,[49] with respect in particular to the transposition of the EU Data Retention Directive into national law.[50] Law providing for the Retention of Telecommunication Data with the intention of investigating serious criminal offences 183(I)/2007 provides in sections 4 and 5 for the access of police officers to telecommunications data. These sections were declared unconstitutional on the basis of article 17 of the Constitution. In a nutshell, the Court held that sections 4 and 5 law 183(I)/2007 were not enacted for the purposes of harmonisation with the Data Retention Directive as they were going beyond its scope and objectives. The Court considered that there was no provision in the Directive requiring Member States to enact legislation enabling access of the police to such telecommunications data, hence sections 4 and 5 law 183(I)/2007 were not covered by the provisions of the Directive and were found inconsistent with article 17 of the Constitution. Article 17 was subsequently amended with the Sixth Amendment of the Constitution Law 51(I)/10, to ensure the compatibility of sections 4 and 5 law 183(I)/2007 with the Constitution, by adding article 17 section 2 (C) as provided above.[51] Following the annulment of the Data Retention Directive by the CJEU in *Digital Rights Ireland*,[52] the Supreme Court considered whether this had any effect upon the validity of law 183(I)/2007.[53] The Supreme Court held by majority that law 183(I)/07 had been promulgated as domestic legislation and accordingly could not be affected by the annulment of the Data Retention Directive.[54]

National security issues do not appear to feature directly in data protection case law as far as the interpretation of constitutional provisions is concerned. The focus is more on

48 Emphasis added.

49 *Matsias and Others* [2011] 1 CLR 152, full bench of the Supreme Court of Cyprus, following *Alexandrou* [2010] 1 CLR 17 (in Greek).

50 For a detailed legal appraisal, see C. Kombos and S. Laulhé Shaelou, 'The Cypriot Constitution under the Impact of EU law: An Asymmetrical Formation' in A. Albi and S. Bardutzky (eds), *National constitutions in European and global governance: democracy, rights and the rule of law*, Asser Press, 2019, pp. 1373-1432, pp. 1412-15.

51 See Emilianides, pp. 182-4.

52 Judgment of 8 April 2014 in Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

53 *Attorney-General v. Isaia*, Civil App. 402/2012, Judgment of 7 July 2014 (in Greek). See however dissenting decision.

54 For a critical approach, see Kombos and Laulhé Shaelou, pp. 1414-15.

the prevention, investigation or prosecution of serious criminal offences and law enforcement. The balancing exercise between fundamental rights (privacy) and national security is however inherent in the Constitution.

With respect to national legislation, it should be noted that section 33(4) law 125(I)/2018 pertaining to administrative offences and sanctions provides that if a person is convicted of committing any of the offences referred to in section 33(4)(1), 'which damages the interests of the Republic or impairs the free governing of the Republic or **compromises national security**,[55] he or she shall be subject to imprisonment which shall not exceed five (5) years or to a fine which shall not exceed fifty thousand (50,000) euro or to both of these penalties.' In the post-GDPR regime, national security therefore appears to constitute an aggravating circumstance affecting the sanction imposed on any controller or processor in breach of this provision.

Law 44(I)/2019 implementing the LED in Cyprus provides in section 4(2) that its scope does not extend to the activities of the Cyprus Intelligence Service and of the Police when pertaining to the protection of national security. Section 15 of the law reproduces article 13 of the Directive on information to be made available or given to the data subject and introduces an exception for national security among others, subject to a proportionality test (section 15(3)(d)). Section 17 of the law reproduces article 15 of the Directive on limitations to the rights of access and introduces an exception to protect national security subject to a proportionality test (section 17(1)(d)). Section 18 of the law reproduces article 16 of the Directive on the right to rectification or erasure of personal data and restriction of processing and introduces the possibility to restrict the obligation to provide information on the refusal to erase on the grounds of national security, subject to the same proportionality test (section 18(7)(d)). Following an assessment of the adequate level of protection of personal data in the third country concerned, including by reference to its national security, law 44(I)/2019 allows in sections 38(2) and section 41 the transfer of personal data to third countries without prior authorisation or in special cases on grounds of serious threats to national security.

In terms of administrative principles, procedures and practice, the powers of the Data Protection Commissioner in Cyprus can be limited on national security grounds under the pre-GDPR law 138(I)/2001. Section 23 provides that national-security-sensitive information can be excluded from the scope of the law (paragraph 1) provided this is documented through a formal confirmation from any Minister or the Attorney General of the Republic of Cyprus that such information need to be excluded, in order to protect national security (paragraph 2), unless such a disclosure would put national security at risk (paragraph 3). Administrative practice also refers to national security as a potential justification – interpreted strictly – for the restriction of privacy in highly risky workplaces,

55 Emphasis added.

such as in the Data Protection Commissioner's Opinion 2/2018 on the use of video surveillance at the workplace and biometric systems[56] and related decisions of the Commissioner.[57]

More generally, national security constitutes an express restriction on the following administrative rules, as expressed in the Law on good administration 158(I)/99: keeping minutes (section 24(4)) and the publication of the due reasoning of an administrative act (confidentiality) (Art 26(4). It should be noted that the publication of personal data constitutes in both cases another exception to the said rules.

Thus, there appears to be no generic definition of national security in the Constitution, legislation or in administrative practice other than the contextual delimitation of public security, defence, State security and the fighting of crime, subject to proportionality. Judicial practice may also be limited in the context of national security per se, for evident reasons, but the increased focus on the protection of personal data at the European level in the last decades, including through the Charter, has no doubt lent a new lens to the contextualisation of law enforcement and/or national security activities at the national level.

The question of the application of the Charter to law enforcement and/or national security activities in Cyprus, in the context of personal data retention, disclosure and protection, has increasingly come to the fore. In an appeal before the Supreme Court of a decision of a lower court to allow the disclosure of personal data (IP address) in the course of criminal investigations as provided by the law, the Court considered the extent to which the *Tele 2 Sverige AB* jurisprudence of the CJEU on the interpretation of article 15(1) of Directive 2002/58, could affect the domestic framework applicable to serious criminal offences in Cyprus (Law providing for the Retention of Telecommunication Data with the intention of investigating serious criminal offences 183(I)/2007 and laws related to child pornography). This was so in view of the fact that the decision of the CJEU was issued after the given order for disclosure and notwithstanding the previous rulings of the Supreme Court in *Matsias* and *Isaia*.[58] As the CJEU recalls, article 15(1) of Directive 2002/58 provides for derogations from the principle of confidentiality of communications and related traffic data 'to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system', or one of the other objectives

56 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3f_gr/page3f_gr?opendocument (in Greek).

57 See 2017 annual report, pp. 57-67 www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/reports_gr/reports_gr?opendocument (in Greek).

58 Appeal 26/2017, *Artemis Kkolos*, judgment of 26 April 2018 (5 judges) (in Greek).

specified in article 13(1) of Directive 95/46.[59] The Supreme Court found that what was at stake was the review of legality of the said order, also vis-à-vis EU law and the Charter in accordance with article 1A of the Constitution, and that the interpretation of the Directive given by the CJEU with respect to the protection of fundamental rights as per the Charter must be treated as if it existed since the inception of the Directive. As stated in *Tele 2 Sverige AB*, it derives that 'the importance both of the right to privacy, guaranteed in article 7 of the Charter, and of the right to protection of personal data, guaranteed in article 8 of the Charter, as derived from the Court's case-law […], must be taken into consideration in interpreting article 15(1) of Directive 2002/58'.[60] The Supreme Court held that *Tele 2 Sverige AB* could affect the legality of the said order to the extent that access was given to personal data retained on the basis of legal provisions which may be incompatible with the Charter but that the review of legality would require the examination of the constitutionality of the legal framework in Cyprus which the Court did not proceed to carry out in this case.

The review of the legality of sections 4(1) and (4) law 183(I)/2007 allowing for the storage of data for six months with no safeguards was conducted by Judge Psara-Miltiadou in an application for a Certiorari seeking to annul disclosure and investigation orders for alleged serious criminal offences.[61] Looking at the case 'from the lens of EU law' and referring to *Tele 2 Sverige AB*, the Judge finds that the protection of telecommunication data is not absolute and that Member States may derogate on the grounds as stated by the CJEU in paragraph 90 of *Tele 2 Sverige AB* (exhaustive list). The orders at stake in the case were found to be quite strict and clearly falling under the category of detection of criminal offences, serious ones. She then turned to the principle of proportionality as examined by the CJEU in *Ministerio Fiscal*,[62] where the CJEU stated that the objective pursued by legislation governing access to data 'must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails' and that 'serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'… By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally'.[63] Linking proportionality to the discretion of the national courts in the process, she refers to two decisions of the Supreme

59 Judgment of 21 December 2016 in Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB* [2016] ECLI:EU:C:2016:970, para. 90.

60 Ibid, para. 93.

61 Application 3/19, *Michael DT*, judgment of 16 January 2019 (in Greek).

62 Judgment of 2 October 2018 in Case C-207/16, *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788.

63 Ibid, paras 51, 56-7.

Court of Cyprus where the proportionality test was applied,[64] and leads to consider whether the interference with articles 7 and 8 Charter was 'serious'. In all three cases the interference with fundamental rights, if any, was deemed not serious.

It appears quite clearly from the above that the courts in Cyprus, who are also responsible for issuing, limiting and/or rejecting access orders to personal data in specific instances of law enforcement, have accepted the application of the Charter to data retention for overriding purposes such as the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. It would be expected that the courts adopt a similar reasoning by analogy for the safeguard of national security, defence or public security. For the moment however, it would appear that the balance between law enforcement or overriding interests vis-à-vis fundamental rights in the field of personal data retention leans towards the former, with not much justification on the basis of the Charter.

64 Appeal 219/15, *Eudoka*, judgment issued on 29 December 2016 and Appeal 51/2017, judgment issued on 14 November 2018 (in Greek).

Czech Republic

Ondřej Serdula and Vojtěch Bartoš[*]

A Setting the Scene

Question 1

The General Data Protection Regulation[1] (hereinafter "GDPR") was implemented[2] into the Czech legal order by two main instruments – Act no. 110/2019 Coll., on the Processing of Personal Data (hereinafter "Data Processing Act"),[3] and Act no. 111/2019 Coll., Amending Certain Laws in Connection with the Adoption of the Act on the Processing of Personal Data (hereinafter "Accompanying Act"). The first thing to note about these acts is that they both entered into force on the 24th April 2019, almost one year after the GDPR. The unexpected delay in the legislative process has led to the undesirable situation in which both the GDPR and the "old" national legislation implementing the Directive on the protection of individuals with regard to the processing of personal data[4] (hereinafter "Directive 95/46") were in force for almost one year. Therefore, the addressees of these norms had to find their way around which of the national rules should be completely disregarded in favour of the GDPR rules and which, on the other hand, should be further applied together with the new directly applicable EU legislation.

The Data Processing Act is divided into five chapters. The first chapter lays down the aim and general scope of the Act. The second chapter implements the GDPR and as such contains only the necessary rules to make the GDPR work within the national context.

---

* Ondřej Serdula is lawyer in the EU Law Department of Ministry of Foreign Affairs of the Czech Republic and Ph.D. student at the Law Faculty of Charles University in Prague. Vojtěch Bartoš is Junior Associate at HAVEL & PARTNERS s.r.o., advokátní kancelář, member of its Privacy Expert Team. Presented views are our own.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 It should be noted that in the Czech context, the term "adaptation" is generally used with regard to adjustment of national legal order to the directly applicable instruments of EU law.

3 The word processing was chosen to distinguish the new legislation from the "old" Act no. 101/2000 Coll., on the Protection of Personal Data, which implemented the Directive 95/46.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

The third chapter implements Directive 2016/680 and as such deals with the processing of personal data for the purposes of prevention, investigation, detection and prosecution of criminal offenses. The fourth chapter regulates the processing of personal data for national security and defence purposes. The last chapter determines the status and the competences of the National Supervisory Authority (hereinafter "NSA").[5]

It is clear from the above-mentioned outline that although all three substantial chapters of the Data Processing Act cover the processing of personal data, each required a completely different approach from the national legislator. For example, while the second chapter needed to be strictly complementary to the GDPR, the third chapter, on the other hand, needed to fully implement the directive and therefore contain all the relevant substantive rules. The fourth chapter then deals with the very specific kind of processing that falls completely outside the scope of the EU law. Therefore, the Data Processing Act contains three very different sets of rules for the processing of personal data, depending on the purpose of the processing. However, this can make the Act itself somewhat difficult to understand for the common citizen.

While implementing the GDPR, the Czech government aimed for a somewhat minimalist approach, clearly stating its goal not to increase the regulatory burden on enterprises and avoid "gold-plating" at all costs. Although it is hard to judge whether the Czech legislation made maximal use of all the possible exceptions provided for in the GDPR, it probably comes very close. It certainly does not make use of any of the possibilities *to increase* such burden.[6] The most important rule in this regard is contained in paragraph 11 of the Data Processing Act. This paragraph allows for restriction of *all* the obligations and rights in articles 12 to 22 GDPR, as well as article 5 GDPR, with regard to *all* kinds of processing, as long as these exceptions represent necessary and proportionate measures to safeguard the interests mentioned in article 23(1) GDPR. To prevent abuse of this general exception, each controller is obligated to report every such restriction to the NSA. Although it may be debatable whether such general exception is in line with the requirements of article 23(2) GDPR, the author considers it completely logical, as it seems practically impossible to *explicitly and specifically* cover all the necessary exceptions for all the possible types of processing in national law. Moreover, the obligation to report these restrictions to the NSA should pave the way to settled administrative practice and case law with regard to the more common types of processing. Most importantly, the Accompanying Act

5 In the Czech Republic, the role of the NSA is performed by the Office for the Protection of Personal Data. Office for the Protection of Personal Data, www.uoou.cz/en/. All webpages referred to were visited 3 February 2020.

6 See, for example, article 9(4), article 37(4) or article 35(10) GDPR.

introduced more precise rules for many types of processing.[7] These will take precedence over the "catch-all exception" contained in paragraph 11 of the Data Processing Act.

The Data Processing Act itself then introduces more concrete exceptions with regard to the processing necessary for compliance with a legal obligation or the performance of a task carried out in the public interest. For instance, it provides for certain simplifications with regard to the information duty of the controller or the exception from the obligation to carry out data protection impact assessment.

The access to official documents within the meaning of article 86 GDPR is covered by Act no. 106/1999 Sb., on the Free Access to Information, which states that access to personal data should be granted only under the specific laws regulating the protection of personal data. However, it also lays down some exceptions to this rule. For example, some personal data about public officials or persons receiving public funding can be provided. The conflict between the freedom of receiving information and protection of personal data is then usually decided by the balancing of conflicting interests in each particular case. Because of that, there is now a rather vast body of case law regarding these issues, with notable cases dealing with access to information about the salaries of public servants, past affiliations of judges with the communist party etc.[8]

The processing of national identification numbers within the meaning of article 87 GDPR is governed mainly by Act no. 133/2000 Coll., on the Evidence of Residents and Birth Certificate Numbers. This act allows for such processing only when it is prescribed by a specific law, necessary for public administration purposes, necessary for exercising legal claims or with the consent of the data subject. Naturally, many laws and regulations require certain subjects (banks, employers, insurance companies) to process national identification numbers. The Czech Constitutional Court also recently annulled the part of the law which required the tax identification number (corresponding with the national identification number) of the seller or service provider to be present on every receipt.[9]

The Data Processing Act does not contain specific rules for the processing of personal data in the context of employment within the meaning of article 88 GDPR, so the general rules of the GDPR will usually apply. Nevertheless, some specific rules for processing can be found in Act. 262/2006 Coll., Labor Codex. For instance, except in some specific cases, the Labor Codex generally forbids secret monitoring of behaviour or communications of employees. It also forbids the employer to require disclosure of information that is not directly related to the employment relationship, again with some minor exceptions. Naturally, several acts of public law also require the employer to carry out the processing

7 For instance, the Accompanying Act contains specific rules for processing of personal data in areas of social security, tax collection, insurance business, medical services etc.

8 Judgment of the Constitutional Court dated 17 October 2017, no. IV. ÚS 1378/16; Judgment of the Constitutional Court dated 8 November 2011, no. IV. ÚS 1642/11.

9 Judgment of the Constitutional Court dated 12 December 2017, no. Pl. ÚS 26/16.

of employees' personal data, even after the termination of the employment contract (for instance for tax or social insurance purposes).

Closely following the wording and logic of article 89 GDPR, the Data Processing Act also introduces general exceptions with regard to processing for scientific, historical and statistical purposes. Processing for archiving purposes is regulated by Act no. 499/2004 Coll., on Archiving, which was amended by the Accompanying Act.

The Czech NSA exercises all the oversight and supervisory competencies prescribed by the GDPR towards all the processing covered by the GDPR, apart from processing operations of courts acting in their judicial capacity and the processing for journalistic, academic, artistic and literary purposes (see below). The NSA can also set the criteria and requirements for the purposes of article 41(3), 42(5) and 43(1) GDPR, adopt standard contractual clauses for the purposes of article 28(8) and 46(2) GDPR and approve codes of conduct for the purposes of article 40(5) GDPR. The Czech NSA also exercises supervisory competences over processing for the purposes covered by the third chapter of the Data Processing Act, except for processing operations of courts and public prosecutor offices. The Czech NSA has no competences over the processing for national security and defence purposes.

Last but not least, thanks to the unexpected MP amendment to the Accompanying Act, the Czech NSA also gained the competence to review decisions of the other public authorities in the area of access to official documents. It remains to be seen how it exercises this new and from a comparative point of view rather unorthodox competence.

Question 2

In the Czech Republic, the catalogue of fundamental rights is not contained in the constitution itself, but in a separate document, the Charter of Fundamental Rights and Freedoms (hereinafter "national Charter"). Protection of the private sphere of the individual is then somewhat scattered among articles 7, 10, 12 and 13 of the national Charter. Article 7(1) of the national Charter, which guarantees the inviolability of the person and privacy, is mostly used in relation to interferences with physical and mental integrity. Articles 12 and 13 then explicitly cover some particular areas of the private sphere, namely the sanctity of home and secrecy of communication. Therefore, the most important with regard to privacy is article 10, reproduced below:

Article 10

1. Everybody is entitled to protection of his or her human dignity, personal integrity, good reputation, and his or her name.

2. Everybody is entitled to protection against unauthorized interference in his or her personal and family life.
3. Everybody is entitled to protection against unauthorized gathering, publication or other misuse of his or her personal data.

The content of article 10 of the national Charter is often being compared to the content of article 8 of the European Convention on Human Rights (hereinafter "ECHR"). However, unlike the Article 8 ECHR, article 10(3) of the national Charter explicitly mentions the protection against unauthorized gathering, publication or other misuse of personal data. Therefore, with regard to differentiating between privacy and data protection, the Czech national Charter goes further than the ECHR, but not as far as the Charter of Fundamental Rights of the European Union (hereinafter "EU Charter"), which gives the right for protection of personal data its own article, name, and also provides some other details, such as rights of the data subject or the need for independent oversight.

In most cases concerning data protection, article 10(3) of the national Charter is referenced as the key right, sometimes treated as sort-of semi-independent "right for informational self-determination". Nevertheless, the actual practice of national courts varies. Article 10 as a whole or other related articles of the national Charter are also sometimes referenced in these cases (for instance article 13 in cases concerning data retention). It is hard to say if these inconsistencies have some real consequences, since none of these rights is absolute and, in the end, the methods for assessing the proportionality of interference or balancing conflicting rights are the same.

In the opinion of the author, the EU Charter did not particularly change the way in which Czech courts approach data protection, since the fundamental rights character of data protection was recognized even before its adoption, be it in the national Charter, the ECHR (as a part of private life) or in the jurisprudence of the Court of Justice of the European Union (hereinafter "CJEU"). Nevertheless, especially higher courts nowadays usually make reference the EU Charter and the relevant jurisprudence of the CJEU whenever the EU law applies. But once again, the actual practice varies, and the courts sometimes reach their own conclusions even in cases where the interpretation of the EU Charter is by no means clear or even where the CJEU would probably reach different conclusions. The Supreme Administrative Court decision on access to information about the salaries of public officials[10] or the latest data retention judgment of the Constitutional Court[11] come to mind. Last but not least, the Constitutional Court maintains that although the Czech national law must be interpreted in line with EU law and the EU Charter, the EU Charter

10 Judgment of the Supreme Administrative Court dated 22 October 2014, no. 8 As 55/2012.
11 Judgment of the Constitutional Court dated 22 May 2019, no. Pl. ÚS 45/17.

alone cannot act as a reference point for assessing the constitutionality of national legal acts.[12]

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The approach of private data controllers to the protection of personal data has long been minimalistic. Arguably that was so mainly due to the limited enforcement activity of the NSA which if a breach of the controller's obligation was found firstly ordered to remedy such breach. Only in a second step if the controller did not comply, the NSA imposed in some cases a monetary sanction (often sanctions of not particularly dissuasive nature). Together with the limited resources of the NSA both financially and personally such system created incentives for the controllers not to pay too much attention and money to the implementation of the data protection legislation. Before the GDPR came into effect (or before it became clear that it would become effective) the interpretation and application of the principles of fair processing, purpose limitation and data minimisation by private controllers was mainly the domain of Czech subsidiaries of multinational corporations which obtained internal rules (including internal data protection directives) from their parent companies and which also 'inherited' the processes of handling personal and other data. Such companies generally complied with the standard level of protection of personal data required by Directive 95/46 also in particular with regard to the principles of fair processing, purpose limitation and data minimisation. That was not quite the case with smaller or local business across the market where the knowledge of the legal regulation of the processing of personal data was rather limited.

A relatively satisfying application of the principle of purpose limitation could be seen even pre GDPR in the HR departments of most controllers (i.e. when processing employees' personal data). The majority of the employees' data were processed for the purposes laid down by the relevant legislation (labour law, social security, health insurance, etc.). Such data were also usually handled with due care. Problems usually arose with regard to the principle of data minimisation (employers often aggregated far more personal data than required by law) and the principle of fair processing and transparency since employees were usually not informed about the scope of the processing (such as transfers of personal data of the employees to other countries in case of multinational corporations).

12 See above-cited Judgment of the Constitutional Court no. Pl. ÚS 45/17, para. 54.

Usually satisfactory (at least in comparison to other data processing) was the application and implementation of all the above mentioned principles with regard to the use of CCTV (typically security cameras in business premises, parking lots, etc.). That was mainly due to the fact that such security surveillance systems had to be notified to the NSA and therefore certain minimal requirements such as complying with the principles of purpose limitation and data minimisation had to be complied with. Also such systems have certain labour law implications and therefore more attention was paid to their compatibility with all legal requirements when installed. Operations of such CCTV systems were moreover repeatedly subject to review by domestic courts which set some border lines for the controllers.[13]

With the GDPR and in particular due to the potentially very high sanctions imposed under it a big part of private data controllers sought out legal help and implemented the fundamental principles of processing of personal data into their processes (the mere fact that the majority of the companies on the market needed to implement even these fundamental principles shows the state of things in the "pre-GDPR era"). Usually the controllers had to newly adopt internal rules and policies for handling personal data, handling the exercise of data subjects' rights (usually no such processes existed, very often in practice the relevant managers were not even aware of such rights or their understanding was somewhat misguided), handling potential data breaches (some rules with regard to general IT security were usually implemented however regardless of the data protection legislation), data retention schemes and related processes for timely erasure of personal data.

Firstly, it must be said that the NSA does not regularly publish its decisions. It only publishes notices and summaries of chosen decisions. The authors therefore use the limited public sources and their professional experience when they refer to the decisions of the NSA.

The NSA has in general in its practice enforced the fundamental principles both pre GDPR and after its adoption. The enforcement of the principles of purpose limitation and data minimisation were probably in the centre of the enforcement activities of the NSA. It can be illustrated on the decision making practice of the NSA related to the personal data published in publically accessible registers such as the land register. It was a common practice in the Czech Republic namely in the construction business that companies offered their goods and services to persons on the basis of records in the land register. The NSA however decided that such personal data cannot be fully used (i.e. not all of the data from the register) for marketing and commercial purposes without further consent of the data

13 One of the cases from the Czech Supreme Administrative Court was submitted to the CJEU as a reference for preliminary ruling on the interpretation of the household exemption in which the Court of Justice issued the judgment of 11 December 2014 in Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů (Ryneš), ECLI:EU:C:2014:2428.

subjects. Such processing would lack a proper legal basis and would be contrary to the principle of purpose limitation and data minimisation.[14] The GDPR made the use of such publically available personal data even stricter since it does not contain any legal basis for such processing compared to the former Data Protection Act.[15] The principle of fair processing is applied and assessed by the NSA together as one with the principles of legality and transparency.

Generally speaking, pre-GDPR the use of personal data as well as any other data by most private controllers was in the Czech Republic governed mostly by their commercial needs and not primarily by the legal principles of processing of personal data. That changed partly with the GDPR which pointed the attention of the relevant managers also to the privacy aspect. On the other hand with the limited resources the NSA has at its disposal it focuses mainly on the application and enforcement of the fundamental principles set out in article 5 GDPR. However, the NSA refuses to take a stricter approach towards the controllers and impose fines in an amount that would be a more persuasive incentive for the controllers to invest into the protection of personal data.[16]

Question 4

Firstly, there is so far no case law of any Czech court to the application and interpretation of the GDPR in that regard. All cases cited relate to the Data Protection Act.

Particularly these two legal bases were most distinctly applied and interpreted by Czech courts in the context of the use of CCTV. In that regard the Czech courts and most notably the Supreme Administrative Court explained that the operation of CCTV cannot be based on the consent of the data subjects but rather on the protection of the legitimate interest of the controller which until then was not properly understood by the recipients of legal norms in the Czech Republic. When assessing the legitimate interest the Supreme Administrative Court used the traditional proportionality test of the Czech Constitutional Court when balancing two fundamental rights. Firstly, the use of CCTV must be suitable

14 Decision of the NSA of 2 September 2014 no. UOOU-06722/14.

15 Section 5 para. 5 of the Act No. 101/2000 Coll., on the protection of personal data and on the amendment of other acts, as amended, allowed the use of contact details obtained from a public register for offering goods or services to the data subjects. The Data Protection Act used to implement the Directive 95/46 and was repealed by the Data Processing Act.

16 The highest penalty ever imposed by the NSA for the violation of the former Data Protection Act or the GDPR was imposed in 2016 on T-Mobile Czech Republic a.s. for a data breach when a former employee stole the database of T-Mobile's clients and the fine amounted to 3.6 million Czech koruna which equals to approximately 140 000 euro. However, such an amount of fine by the NSA is indeed extraordinary. Since the GDPR came into effect the NSA imposed nine fines in total where six fines were in the amount of approximately 200-1150 euro, one fine in the amount of 3000 euro and one fine in the amount of 10000 euro. Such amounts are much more illustrative of the practice of the NSA.

in order to achieve the pursued fundamental rights of the controller. Secondly, the use of CCTV must be necessary in order to achieve the pursued aim. Thirdly, the importance and gravity of the two fundamental right standing against each other must be assessed in the light of the factual circumstances of the case at hand (balancing *stricto sensu*).[17] In other words when the processing of personal data is to be based on the legitimate interest, a test of proportionality must be carried out.[18]

The Data Protection Act established the consent as the principal legal basis for any processing of personal data from which other legal basis were merely an exception. As such the consent was also applied by the courts and the exceptions to the principle were to be interpreted narrowly. The right not to have personal data processed without consent was interpreted to be a part of the right to the informational self-determination protected by the Czech constitution, the right to private and family life protected by article 8 ECHR and hence more broadly a part of one's integrity as a fundamental precondition to a dignified existence.[19] Regardless of the change in the text of the relevant legal norm (the GDPR formulates the different legal basis as equally valid) the aim and purpose of the consent of the data subject remains and the Supreme Administrative Court itself noted that the GDPR if applicable at the case at hand would not change its conclusions.

When interpreting the terms "consent" and "legitimate aim" the Supreme Administrative Court adopted the relevant case law of the ECJ as well as the opinions of the Article 29 Working Party an interprets these notions in their light.

Question 5

When entering the office, the chairwomen of the NSA issued a statement that personal data and the right to have them protected is a fundamental and hence inalienable right. However, there are decisions of the NSA which in fact allow trading of personal data for a service.

In particular this practice developed in the context of loyalty programs which are very common, process extremely large amounts of consumers' personal data and became one of the basic sources of business data for undertakings. Some controllers (most often

17 In its further case Law the Supreme Administrative Court explicitly refers in that regard to the analogical case law of the Court of Justice, namely judgment of 24 November 2011 in Joined Cases C-468/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and C-469/10, Federación de Comercio Electrónico y Marketing Directo (FECEMD), ECLI:EU:C:2011:777, judgment of 19 October 2016 in Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland (Breyer), ECLI:EU:C:2016:779, judgment of 4 May 2017 in Case C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme", ECLI:EU:C:2017.

18 To that end see e.g. the judgement of the Supreme Administrative Court from 25 February 2015 no. 1 As 113/2012.

19 See in particular the judgement of the Supreme Administrative Court from 19 April 2018 no. 2 As 107/2017.

companies selling consumer goods but also e.g. public transport companies) offer their customers to become members of the loyalty program which gives the customer the possibility of buying goods and services with discount, obtaining gifts and other benefits. The terms and conditions of these loyalty programs mostly contain clauses regarding the processing of personal data. Some of these programs present the processing of personal data as based on the legitimate aim of the controller (processing being necessary for the existence of the loyalty program), some of them process the clients' personal data on the basis of a contract (on the membership in the loyalty program) and other base the processing of the personal data on the clients' consent which is then a necessary prerequisite to the membership in the loyalty program.

Admittedly the decision making practice of the NSA in this regard is not very extensive or unified. In the past the author in his practice came across opinions of the members of the NSA who refused the consent as a basis for such processing of personal data with the argumentation that such consent could not be regarded as freely given. On the other hand the NSA issued a decision regarding the loyalty program of the Czech national railway company which subjected the membership with two separate consents with processing of personal data both for strictly marketing and individualised marketing purposes. In that decision the NSA in principle stated that the membership in the loyalty program is entirely voluntary for the customer who is not obliged in any way to take part in it. Also, according to the NSA, not being a member of the loyalty program does not limit the customer in using the services of the controller (i.e. mainly traveling by train). In the NSA's opinion the special prices and other special offers on the services of the controller are entirely in the discretion of the controller and the customer cannot demand them. It is therefore for the controller to decide under which conditions it will offer such benefits to its customers including the requirement of processing of their personal data for marketing purposes.[20]

Question 6

The measures envisioned in article 22(2)(b) GDPR were introduced to several specific laws through the Accompanying act. The automated decision-making and/or profiling is allowed by law in the following areas: tax and duties collection, social security, medical insurance, building and retirement savings, capital markets, financial crisis prevention and gambling oversight. Generally, the automatic processing is by law allowed in situations where the controller has to regularly issue a vast amount of rather trivial "decisions" (for example, the yearly valorisation of pensions) or when automated processing and/or profiling seems necessary to safeguard some important interests of state in the modern context (for example,

20 Decision of the NSA in the case no. UOOU-10668/18.

using advanced data analytics for combatting tax fraud). Although the public authorities still employ these methods rather rarely, their usage is expected to increase in the following years with technological developments.

As for the safeguards, the controllers and processors are required to describe the relevant algorithms and selection criteria in the records of processing activities and store them for at least one year after the processing. It is also generally forbidden to issue "true administrative decisions" within the meaning of Act no. 500/2004 Coll., Administrative Procedure Code, based purely on automatic decision-making. Although the objection of the data subject does not preclude further processing in these cases, the controller or the processor is obliged to mark such personal data until the objection is resolved. Other safeguards contained in the GDPR will generally also apply.

Question 7

On 25 January 2019 the NSA published a short notice regarding an inspection of the controller Seznam.cz which is the second largest search engine in the Czech market after Google with a market share around 25%. According to the notice the inspection was focused on the exercise of "the right to be forgotten". The NSA found that all processes of the controller when rights of data subjects under article 17 GDPR are exercised towards the controller comply with the requirements of the GDPR.

In practice also other engines respond when data subjects exercise their rights. So far to the best knowledge of the authors there has been no court litigation regarding "the right to be forgotten" in the Czech Republic.

Question 8

In the Czech Republic, both the freedom of expression and the right to protection of personal data are protected on the constitutional level, so the conflict between them is usually resolved by a classic balancing rights test, considering all circumstances of each particular case. Case law in this area, which often stems from civil law disputes concerning media interference with personality rights of celebrities and public officials, closely follows the jurisprudence of the ECHR in these types of cases. The public law regulation of media also contains some specific legal institutes to remedy the interference with the privacy of persons, such as the right to request publication of reaction or additional information. The most serious interferences can also be dealt with under criminal law.

Interestingly enough, the previous Data Processing Act did not state any explicit exceptions with regard to freedom of expression. Therefore, in theory, all the data protection rules applied also on data processing for journalistic purposes. In reality, this would

disproportionately hinder all journalistic activities. Therefore, the NSA decided to enforce the data protection rules in these cases much more reservedly in an effort not to disturb the above-mentioned balance between the freedom of expression and the protection of personal data.[21]

The lack of concrete rules for the reconciliation of these interests was meant to be remedied by the Data Processing Act. Following discussions about various options with media representatives and the NSA, the government proposal contained some specific exceptions from the GDPR rules for the processing for journalistic, academic, artistic and literary purposes. The goal of these exceptions was to ensure that the duties of the controller and the rights of the data subject cannot disproportionately hinder the freedom of expression. For instance, the duty of the controller to inform the data subject (about the identity of the controller, identity of its source and some other details about the processing) or some rights of the data subject (to access, rectification, restriction of processing or right to object) were in some way limited.

Nevertheless, the main goal of these exceptions was the *adequate balance*, so the duties of controller or rights of the data subjects were generally not completely negated. They were often only postponed, or they could be realized in some different way (for instance, the information duty could be fulfilled by providing information about the general types of regularly performed processing on the controller's website). The extent of these exceptions was also meant to reflect various stages of journalistic work (for instance, limitations of data subjects' right to access would be different before and after publication).

This approach was however met with great caution in the Czech parliament. Members of the Parliament worried that these exceptions were to casuistic and that such approach might lead to undesirable restrictions on the freedom of speech. In the end, the proposed casuistic exceptions have been preserved, although some with different wording. More importantly, the parliament also introduced a new *general exception* for the purposes of journalistic, academic, artistic and literary processing. According to this general exception, articles 5, 12 to 22, 33, 34, 56 a 58(1)(a),(b),(e),(f) and 58(2)(d),(f)(g) and chapters II, IV, V and IX of the GDPR do not apply, apply proportionally or their use can be postponed if it is necessary for the above-mentioned purposes. Chapter VII of the GDPR does not apply at all. Application of some of these exceptions is however limited to cases where it is unlikely to result in a high risk to the legitimate interests of the data subject.

Of course, such exception is extremely wide and vague. It is also quite poorly worded, so its relation to the specific exceptions carried over from the government proposal is very unclear. It seems that, in reality, all the actual balancing was once again left for the administrative and judicial practice. This by itself does not pose an insurmountable problem, since it is basically just a continuation of the previous state and prescribing the exact criteria

21 Office for the Protection of Personal Data, Opinion no. 5/2009, www.uoou.cz/files/stanovisko_2009_5.pdf.

for the proportionality test in law is tricky anyway. Nevertheless, it is hard to see the logic behind many of the exceptions, especially those from chapters VII and IX of the GDPR.

As mentioned above, the Data Processing Act entered into force quite recently, so it remains to be seen how these exceptions are interpreted and applied in practice.

C Domestic Enforcement of Data Protection Law

Question 9

The NSA and the only responsible administrative authority enforcing the GDPR in the Czech Republic is the Office for the Protection of Personal Data seated in Prague. The NSA is established by law (formerly by the Data Protection Act and nowadays by the Data Processing Act) which guarantees its formal and functional independence from the rest of the executive branch.

The NSA has its own chapter in the state budget. The Chairperson is appointed and dismissed by the President of the Republic on the basis of a proposal of the upper chamber of the Parliament – the Senate. The Chairperson and the Vice-Chairpersons have to fulfil some relatively strict requirements such as 40 years of age, both moral and criminal integrity university education in the field of law or informatics, necessary knowledge of English, German or French language and at least 5 years of practice in the field of data protection or human rights. Different university education is also permissible if the person has at least 10 years of relevant practice. The function of the Chairperson is incompatible with the function of a member of the Parliament, judge, public prosecutor, or any other position in the public administration and with the membership in any political party. The NSA has two Vice-Chairpersons who are elected and dismissed on the basis of the Chairperson's proposal by the Senate. The NSA has further 7 inspectors who are appointed by the President of the Republic on the basis of a proposal of the Senate for 10 years. Inspectors have teams of co-workers on the executive level.[22]

It exercises all the competences given to the NSA by the GDPR and beyond that it also exercises the competences of the NSA within the meaning of Directive 2016/680.[23] However, it does not exercise these competences towards courts and public prosecutors which are supervised within the structure of the courts or public prosecutors. Further it also compiles

22 Section 50 to 53 Data Processing Act.

23 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

and publishes an annual report on its activities, ensures fulfilment of requirements following from international treaties binding the Czech Republic, and from directly applicable law of the EU and issues, on its own initiative, opinions to the Parliament, on the proposed legislation in the field of personal data protection, if such legislation is not proposed by the Government.[24]

The NSA so far conducted approximately 53 inspections under the regime of the GDPR, imposed 8 fines where the lowest was approximately 200 euro and the highest approximately 10 000 euro.[25]

Question 10

The strategy for complaint-handling of the NSA is partly set by the legislation which requires the NSA to have a yearly inspection schedule. The NSA then responds with the rest of its capacities to the individual complaints and queries via its FAQs, a Basic Handbook on the GDPR which was issued by the NSA and of course where necessary by assessing individual complaints and if found appropriate initiating administrative proceedings against the respective controller.

However, the NSA has not published any long-term complaint-handling strategy or other information related to the key how it divides its resources.

Question 11

The Data Protection Act already offered the possibility (or rather obligation) of the NSA to impose a corrective measure before it would impose a fine. It is therefore a standard practice of the NSA even under the GDPR that it considers the gravity of the violation of the GDPR and if possible it firstly imposes a corrective measure on the controller rather than a fine (prompts the controller to remedy the situation immediately). Only if the violation cannot be corrected, is grave or repeated, the NSA imposes a financial penalty.

The NSA indicated long before the GDPR became effective that it will not impose any drastic sanctions under the GDPR as it was the general (mis)understanding namely of articles 83(4) and (5) GDPR among the public. The NSA expressed through media and other public channels that it considers the high sanction of 10 million euro or 20 million euro respectively and the sanctions based on the turnover to be meant namely for large multinational controllers and that it will more or less continue to impose fines up to 1 000

24 Section 54 of the Data Processing Act.

25 Information from the website of the NSA, www.uoou.cz/ukoncene-kontroly/ds-5649/archiv=0&p1=1277 and www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5546&n=poskytnuti%2Dpravomocnych%2Drozhodnuti%2Dprikazu%2Dza%2Dporuseni%2Dgdpr&p1=1059.

000 Czech koruna (approx. 386,000 euro) which was the upper limit under the Data Protection Act.

Given the relatively dramatic coverage of the GDPR in the Czech media before 25 May 2018 bordering sometimes with hysteria and at that time also no prospect of the implementing national act being adopted soon the NSA presented that it wants to serve as a place for consultations, help and support for the controllers and that it will be rather lenient when assessing the violations and imposing any sanctions (at least for some time after the effective date of the GDPR).

Question 12

The Czech legal system has historically known the concept of damages for intangible harm. Neither the Data Protection Act nor any other act however provided a specific damages claim for a wrongdoing in the field of protection of personal data. As far as the authors are aware there was no case in the Czech Republic in the "pre-GDPR era" where the courts would adjudicate on such a claim brought under the general regime of damages provided for by the Civil Code. Also we are not aware of any damages case brought to the Czech courts under article 82 GDPR.

Until 2014 when the new Civil Code[26] was adopted in the Czech Republic the damages for intangible harm (in particular for personal injury) were strictly set by a Ministerial Decree which provided a specific amount of damages for a particular type of personal injury regardless of the circumstances of the individual case (set amount of damages for e.g. a broken finger regardless of whether it was a finger of a piano virtuoso or a finger of a parking lot guard). The new Civil Code to the contrary brought the (elsewhere not that new) idea that damages for personal injury must be assessed by the courts individually in the light of the particular case at hand. As a reaction to the new situation however the Supreme Court reacted by issuing methodological guidelines for the assessment of damages for personal injury which again brought back many of the elements of the former Ministerial Decree.[27] There is also in the Czech Republic a Government Regulation on the Compensation of Work Injury or Occupational Disease which implemented the very same approach as the former Ministerial Decree.[28]

The compensation of intangible harm is therefore an area where there is no reliable long-standing line of case law and the Czech courts are in general rather reluctant to award high compensation for intangible harm. In the opinion of the authors it will require a

26 Act no. 89/2012 Coll., the Civil Code, as amended.
27 Accessible in Czech, https://is.cuni.cz/webapps/zzp/download/150027990.
28 Accessible in Czech, www.zakonyprolidi.cz/cs/2015-276.

significant amount of time until it becomes clear how the courts will approach the claims brought under article 82 GDPR.

Question 13

The Czech law provides the possibility for data subjects to be represented by an NGO in both civil and administrative proceedings. This is an exception to the general rule in which only a natural person can act as such representative. However, there were already some other areas of law where representation by an NGO was possible, mostly because it was required by other EU law instruments (for instance in discrimination, consumer protection and asylum cases).

To represent the data subject in court proceedings, the NGO must have the protection of data subject rights listed as one of its activities in the founding document and must not distribute its profits. Moreover, the person acting on behalf of the NGO in the proceedings must have full legal education (there is no such requirement if the data subject decides to be represented by natural person). There is no possibility for NGO's to act by themselves within the meaning of article 80(2) GDPR.

There are some NGO's active in the field of data protection in the Czech Republic.[29] Their activities include public information campaigns, submissions of comments on draft legislation, granting awards and anti-awards, representing data subjects and even initiating the constitutional review of the data retention legislation through MP's.[30] The Author is not aware of any personal data cooperatives or unions in the Czech Republic.

Question 14

No formal platform for a regular cooperation of these bodies or regulators has been established.

If any such cooperation exists it will be based almost entirely on personal relationships between the individual officials or employees of the respective bodies and regulators.

29 Iuridicum Remedium, www.iure.org/EN; Data Protection Society www.ochranaudaju.cz/.

30 Share Safely, www.sdilejbezpecne.cz; Big Brother Anti-award https://bigbrotherawards.cz/.

D Data Processing for National Security Purposes

Question 15

The Czech legal order does not contain a clear definition of "national security". For the purposes of this report, the notion of national security is perhaps best understood in connection with the tasks of Czech intelligence services, as they are defined in the Act no. 153/1994 Coll., on the Intelligence Services of the Czech Republic. According to this act, the tasks of the intelligence services include gathering and analysis of information:

- about intentions and activities directed against the democratic foundations, sovereignty and territorial integrity of the Czech Republic
- about foreign intelligence services
- about activities endangering state secrets
- about activities whose consequences may jeopardize the security or significant economic interests of the Czech Republic
- about organized crime and terrorism
- important for the defence and security of the Czech Republic

The notion of public security is therefore quite extensive, including also the issues of combatting organized crime and terrorism or safeguarding significant economic interests of the state.

As mentioned, chapter IV of the Data Processing Act governs the processing of personal data for these purposes. Its rules are however only subsidiary to specific laws governing the activities of individual intelligence services. Understandably, the competences of controllers and processors are generally much wider and the data subject's rights much more limited in this area. Although the GDPR did not have any impact on the processing of personal data in this area, some changes are expected to come in reaction to the revision of the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in near future.

National authorities did not accept the view that the conclusions of the Tele 2 and Watson judgment[31] apply on data retention for national security purposes. In fact, the Czech Republic actively argues against this view in several ongoing CJEU cases.[32] In the view of the Czech government, even if EU law were to apply to such processing, the

31 Judgement of 21 December 2016 in Joined Cases C–203/15 and C–698/15, Tele2 Sverige v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others (Tele 2 and Watson and others), EU:C:2017:214.

32 See ongoing cases C-623/17, Privacy International, C-511/18 La Quadrature du Net and Others and C-520/18, Ordre des Barreaux Francophones a Germanophone and Others.

conditions for proportionality would need to be vastly different from joined cases C–203/15 and C–698/15, *Tele 2/Watson*, due to the different nature of threats against national security and instruments needed to prevent these threats.

However, it should also be noted that the Czech Constitutional Court recently ruled that the general data retention obligation is in accordance with the Czech constitution, even for the purposes of prevention, investigation, detection and prosecution of criminal offences.[33]

33 See above-cited Judgment of the Constitutional Court no. Pl. ÚS 45/17.

Denmark

Søren Sandfeld Jakobsen[*]

A Setting the Scene

Question 1

In Denmark, Regulation (EU) 2016/679 (the General Data Protection Regulation, hereinafter "GDPR") is implemented in Act no 502 of 23 May 2018 on Data Protection (in Danish: "databeskyttelsesloven").[1] The Data Protection Act (or "the Act") is based on Report no 1565 on GDPR and the Legal Framework for Danish Law (hereinafter "the Report").

Although a regulation, GDPR offers considerable flexibility in that it stipulates that Member States in several situations may or even shall adopt national rules. These national rules may either specify a given rule in GDPR, make use of an option which has been left to Member States, adopt exceptions to certain rights or obligations in the GDPR, or carry out certain tasks or actions imposed on Member States under the GDPR.

The Data Protection Act (and the Report and preparatory works to the Act) reflects the flexibility under the GDPR very carefully. With regard to the vital provisions regarding lawful processing, for example, the authorization to specify in national law certain provisions in articles 6 and 9 has partly been utilized, cf. sect. 6-7 of the Act. Other examples cover article 87 regarding processing of national identification numbers (cf. sect. 11 of the Act) and article 88 regarding processing in the context of employment (cf. section 12). In respect of options, examples cover article 8, paragraph 1, concerning a child's age when providing a consent (cf. section 6, paragraph 2 and 3), and article 83, paragraph 7, concerning fines imposed on public authorities (cf. section 41, paragraph 6, of the Act). Articles 23 and 89 authorize (subject to certain conditions) Member States to restrict by way of legislative

* Professor of the law of property and obligations, Copenhagen Business School; attorney at Gorrissen Federspiel, Copenhagen (Denmark).

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119/1. Legal literature on Danish law on the protection of personal data since the coming into force of GDPR: P. Blume, *Den nye persondataret*, 2nd Ed, Copenhagen, Djøf forlag, 2018; N.P. Langemark & J. Dall, *Persondataforordningen – en håndbog for praktikere*, 2nd Ed, Copenhagen, Ex Tuto Publishing, 2019; J. Trzaskowski & M.G. Sørensen, *GDPR Compliance: Understanding the General Data Protection Regulation*, Copenhagen, Ex Tuto Publishing, 2019.

measure the obligations and rights provided for in a number of provisions in the GDPR, and this opportunity has been utilized various places in the Act. As example of certain tasks which the GDPR imposes on Member States can be mentioned article 43 regarding accreditation of certification bodies (cf. section 23 of the Act), and article 51 regarding the supervisory body, cf. Part VI of the Act.

The national supervisory authority in Denmark, the Danish Data Protection Agency (In Danish: "Datatilsynet") supervises the adherence with the Data Protection Act in a similar way and with similar means as the supervision of the GDPR, cf. chapter VI of the GDPR.

In addition to the guidelines from the European Data Protection Board (hereinafter "EDPB"), Datatilsynet also issues guidelines on the interpretation of the most significant rules under the GDPR.[2] The guidelines are not as such legally binding, as they only express the opinion of Datatilsynet itself, not the courts. However, legal practitioners usually attach considerable importance to the guidelines.

Question 2

The Charter of Fundamental Rights of the European Union (hereinafter "Charter") is part of the EU Treaty, cf. article 6(1) of the Treaty of the European Union, and as such also a part of the Danish legal order. In that respect, Danish law differentiates between article 7 (the general right to protection of privacy) and article 8 (the specific right to protection of personal data). However, there is not yet any indication in Danish case law that article 7 of the Charter has directly influenced the interpretation of national Danish law.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The basic principles of Directive 95/46/EC have been maintained – and even strengthened and specified – under the GDPR.[3] The principle of "fair processing", which was previously found in article 6(1)(a), in the Directive, now follows from art. 5(1)(a) GDPR. In general,

2 Datatilsynet, www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/, visited 1 February 2020.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.

there is very little case law from the courts in Denmark regarding the Data Protection Directive, and so far no case law regarding the GDPR. Consequently, Danish law in this area is mainly being developed by the NSA, Datatilsynet. That goes for the principle of "fair processing" too. Over the years, Datatilsynet has regularly referred to the principle as part of the basis for the decisions and opinions.

As examples can be mentioned the requirement of providing prior information to the data subjects at the time of coordination for control purposes, the requirement of notice to staff, etc. on television monitoring of jobs before monitoring commences, the restrictions on the use of credit information in connection with job recruitments, and the duty to note if a registered person has objections against the accuracy of registered personal data.

Furthermore, Datatilsynet has established that where personal data due to a security breach has been disclosed to unauthorized persons, it will - depending on the specific circumstances - result from the requirement of fair processing that the data controller shall notify those concerned people. In addition, Datatilsynet has prepared guidelines on accidental disclosure of personal data on the Internet that it is a manifestation of the requirement of fair processing. It follows from the guidelines that data controllers must seek to limit the damage in such instances, which includes removing the information from the website as soon as possible, informing the persons concerned of the error, and investigate whether the information is found on search engines and, if so, seek to have it removed.

The principle of purpose limitation is also well-known from the 1995 Directive (article 6(1)(b)). In the only reported court case, the Eastern High Court stated that a real estate agent who used his access to a credit information system to obtain and pass on information about a local politician's unpaid debt, was violating the principle of purpose limitation.[4] There is an extensive practice from Datatilsynet on the principle. The core of this practice is, that the data controller shall state a purpose which is sufficiently defined and delimited, that the processing of personal data shall be for legitimate purposes only, and that subsequent processing may not be inconsistent with the purposes for which the data were originally collected.

From Datatilsynet's practice can be mentioned a case involving the processing of personal data in connection with an insurance case.[5] In the case a policyholder complained to Datatilsynet about his insurance company's processing of personal data in connection with a video recording and observation as part of the insurance company's treatment of a claim for damages raised by the policyholder. Among the information gathered was information on the complainant's conduct inside his house. Datatilsynet held that recordings and observations inside a person's home in the manner in question under the

4 Cf. the Danish Weekly Law Reports 2004, p. 2204.

5 Case 2014-213-0047.

circumstances might be justified in order to fulfill the stated purpose. However, there was no information on whether the policyholder was doing something in the house that could be relevant to the insurance case. Against this background, Datatilsynet found that registration of the observation monitoring in question went beyond the purpose with the monitoring, and thus was not compatible with the principle of purpose limitation.

The principle of "data minimization" in article 5, paragraph 1, litra c, corresponds with the principle of proportionality in article 6(1)(c) of the 1995 Data Protection Directive. There appear to be no reported court cases regarding the interpretation of the principle, but Datatilsynet has applied it in a number of cases. As an example can be mentioned a case concerning electronic transfer of property information from a municipality to an energy company, where Datatilsynet stated that the municipality should take measures to ensure that the energy company was only given access to the information that the energy company should use for calculation of a statutory heating duty.[6]

In a case concerning a municipality's transfer of social security numbers to a housing company, Datatilsynet stated that the municipality should not disclose information about social security numbers to the private housing company as part of their communication. Disclosure of social security numbers should only be done for the purpose of identifying tenants receiving housing support. Information of tenant numbers would be sufficient identification information.[7]

Question 4

There is an extensive practice from Datatilsynet regarding the interpretation of the notions of "consent" and "legitimate interest", but only a few court cases.

In the only reported case concerning consent, the Supreme Court stated in a decision from 2011 that an unspecified consent to a potential new employer to collect references from a former employer could not cover the collection of highly sensitive personal data, e.g. regarding a possible alcohol abuse.[8]

With regard to "legitimate interest", no reported court practice exists. However, there is a rich volume of case law from Datatilsynet.[9]

---

6 Case 2003-323-0101.

7 Case 2003-323-0109.

8 Cf. the Danish Weekly Law Reports 2011, p. 2343 H.

9 The comprehensive case law is thoroughly reviewed in H. Waaben & K. Korfitz Nielsen, *Lov om behandling af personoplysninger med kommentarer*, 3rd Ed, Copenhagen, Jurist- og Økonomforbundets Forlag, 2015, pp. 229 et seq.

Question 5

There is no evidence of any heated debate, or any decisions, in Denmark regarding the validity of personal data as "counter-performance" for the provision of digital content. The issue relates to the question whether a consent has been given voluntarily. In its guidelines on the notion of consent, Datatilsynet notes, that if a contract, e.g. regarding access to digital content, is conditioned on consent, the greatest possible consideration must be given to whether, among other things, the fulfillment of a contract is conditional upon consent to the processing of personal data which is not necessary for the performance of the contract.[10] In other words, it means that consent is not considered to have been given voluntarily if, e.g. purchase of a product or service depends on consent, although such consent is not necessary for the purchase of the product or service. This is in line with article 7(4) and article 6(1)(b) GDPR.

Question 6

Article 22(2)(b) GDPR is basically regarded a continuation of the 1995 Data Protection Directive's article 15(2)(a). Denmark has in a number of situations introduced legislative measures pursuant to the provision. An example is the legislation on student grants, which prescribes that an application for a student grant must be provided via a fully digital and self-serviced system that renders an automated decision. This legislative measure is considered compliant with article 22(2)(b) GDPR, because the automated decisions can be brought before a board of appeal. Another, very similar, example of a national legislative measure is the set-off of a person's debt to a public authority, which can be recovered via a fully digital system. Automated decisions from the system can be brought before a board of appeal in a fast-track process.[11]

There is no court practice on the subject.

Question 7

The right to erasure in article 17 GDPR, and its predecessor in the 1995 Data Protection Directive, article 12, has not been applied by Datatilsynet or the courts. No Danish domiciled search engines exist.

10 Guidelines on Consent, November 2017, pp. 5-6.

11 See more detailed the Report, pp. 380 et seq.

Question 8

Article 85 GDPR provides that

> "Member States shall … reconcile the right to the protection of personal data … with the right to freedom of expression and information, including processing for journalistic purposes …".

The Data Protection Act, like its predecessor, The Personal Data Act from 2000, transposes article 85 by entirely exempting from the scope of the Act (and thus the GDPR) processing of personal data for journalistic purposes and journalistic databases, cf. section 3, paragraphs 4-8.

Further, according to the Act, section 3, paragraph 1, the Act does not apply if this would result in a violation of freedom of speech and freedom of information. The provision refers to article 10 of the European Convention on Human Rights and article 11 of the Charter, and it serves as a reminder that freedom of expression must be taken into consideration when interpreting the data protection rules.

Datatilsynet has decided some cases, citing the provision (in the previous act). In one case, the Danish People's Party's webpage published the names and districts of 3,218 persons who were granted Danish citizenship, including comments that some of them were criminals. As the names were already published in connection with the granting of citizenship, this publication was not violating the Act, and the comments fell within the protected area for freedom of speech.[12]

In the second case, a company had published the name, position and workplace of a public employee working for the Danish Working Environment Service and commented his visit to the company. The Board found the mentioning acceptable, as it was a part of a public debate.

In a later case, "The Black Register" ran an open webpage featuring names, job title, work phone of public servants under the headings "neglect of duty" and "abuse of power".[13] Sometimes also date of birth and political affiliation were added to the personal data. The Board dismissed the case, referring to what is now the Act, section 3, paragraph 1, arguing that it was part of a public debate with a mere voicing of opinions.

12 DT 2000-216-0005.
13 DT 2011-215-0874.

C Domestic Enforcement of Data Protection Law

Question 9

Pursuant to Part VI of the Act, corresponding with Chapter VI of the GDPR, the primary relevant public authority in Denmark is Datatilsynet (the Danish Data Protection Agency), which supervises compliance with the data protection rules, provides guidance and advice, deals with complaints, makes inspections and issues responses to draft legislation etc. It follows from sect. 37 of the Act that the Court Administration in accordance with Chapters VI and VII of the GDPR supervises the processing of data carried out for the courts when they do not act in their capacity of courts. In respect of other processing of data, the decision must be made by the relevant court.

Datatilsynet is independent of Government and Parliament and consists – as before the GDPR – of a Council and a Secretariat. The Council decides in leading cases, while the Secretariat handles day-to-day cases and matters. The Council is appointed by the Minister of Justice and consists of a chairman, who must be a high court judge or Supreme Court judge, and of seven additional members. All members are appointed based on their professional qualifications, and an appointment lasts 4 years, with the possibility to be reappointed once.

The Secretariat consists of a Director and a staff of approximately 60 employees. There are no special rules or policies regarding the employment process of the staff. The staff is composed so that it comprises both legal and IT skills and competences. Both the members of the Council and Secretariat are subject to confidentiality obligations.

Datatilsynet's powers correspond essentially with the GDPR. No additional powers have yet been given, cf. article 58(6) GDPR, but section 35 of the Act authorizes the Minister of Justice to allocate additional powers to Datatilsynet. The authorization has not yet been utilized.

According to its latest annual report and statements to the press, Datatilsynet has experienced a very significant increase in the case-load after the coming into force of the GDPR, notably with regard to cases concerning notification of a personal data breach. In general, Datatilsynet expects three to four times more cases under the GDPR than before.

With regard to the significantly increased level of fines, Datatilsynet has referred two cases to the police with the view to criminal prosecution after the GDPR entered into force on 25 May 2018. In the first case, following an inspection by Datatilsynet in October 2018, a taxi company was reported to the police and Datatilsynet recommended a fine of DKK 1.2 million for violation of the GDPR.

The inspection was focused on whether the taxi company had retention and deletion policies in place in accordance with article 5(1)(e) GDPR, and whether such policies were

complied with internally in the company. Datatilsynet found that the taxi company had only implemented superficial procedures that did not ensure compliance with the requirements of data retention and deletion as set out in the GDPR. This conclusion was primary based on the premise that the taxi company claimed to anonymize personal data after a 2 year retention period by deleting only the name of data subjects, and by deletion of telephone numbers only after a period of 5 years. At the time of the inspection, the taxi company had information about 8,873,333 taxi trips, which were older than 2 years. The case has not come to trial yet.

In the second case, Datatilsynet reported in June 2019 a furniture outlet business to the police and recommended a fine of DKK 1.5 million for not having deleted personal data concerning 385,000 customers which were no longer relevant. The case has not yet come to trial.

Question 10

There is no published strategy from Datatilsynet regarding their complaint-handling. However, as mentioned Datatilsynet has experienced a very significant increase in incoming cases, including complaints, after the entry into force of the GDPR. This is forcing Datatilsynet to be very selective when deciding what cases to pursue or not. Under article 57 GDPR, if a complaint is "manifestly unfounded or excessive", the supervisory authority can refuse to act on the complaint. Danish law places no constraints on such approach.

Question 11

The power to impose corrective measures, cf. article 58(2) GDPR, largely corresponds with applicable Danish law before the GDPR. Under Danish law, and in accordance with article 83(9) GDPR, Datatilsynet can as a main rule not impose administrative fines, only the courts can do that.

With regard to the enhanced administrative fines under the GDPR, this is an innovation under Danish law, where the fines previously have been rather low, not more than DKK 5-25,000. As described above, two court cases are pending under the GDPR with the allegation of fines of more than DKK 1 million. Under Danish law, fines can also be imposed on public authorities.

Denmark has not utilized the possibility to impose "other penalties" subject to article 84 GDPR. Hence, the sanctions according to Danish law correspond with the GDPR.

Question 12

Denmark has historically awarded damages for intangible (i.e. non-economic) harm, and this is regarded to apply to intangible harm under data protection law, too. The legal basis for awarding intangible harm is found in section 26 of the Civil Liability Act (in Danish: "erstatningsansvarsloven") concerning infringement of other people's "freedom, privacy, honor or person".[14] Only infringements of some severity are covered by section 26. The awarded damage pursuant to section 26 is assessed based on an estimate and is normally relatively low.

From case law can be mentioned a judgment from the Maritime and Commercial Court concerning an employer's TV monitoring of an employee in a store.[15] The monitoring took place from the employer's private residence in one half an hour to three quarters. The surveillance was not work or safety-related justified and resulted in the collection of personal data (images) in violation of the Personal Data Act then in force. The employee was awarded DKK 25,000 in compensation under section 26 of the Civil Liability Act.

In a decision from 2011, the Supreme Court ruled that a municipality's disclosure of information on suspicion of alcohol abuse as part of a potential employer retrieval of reference information was an unlawful disclosure under the Personal Data Act.[16] The Supreme Court did not consider that the employer would have obtained the employment if the information had not been disclosed, so there was no basis for damages for an economic loss. However, the employee was awarded DKK 25,000 pursuant to section 26 of the Civil Liability Act.

In a judgment from 2005, the Western High Court took a position on an employer reading an employee's private email correspondence, which resulted in an unjustified termination of employment.[17] The court found that the employer was accidentally acquainted with the e-mail correspondence, and that without reading the correspondence it was not possible to find out that it was private. There was therefore no violation of the employee's rights which could form basis for compensation under section 26 of the Civil Liability Act. Since the employee had not suffered any financial loss, there was no basis for damages pursuant to the Personal Data Act either.

14 Consolidated Act no 1070 of 24 August 2018.
15 Cf. The Danish Weekly Law Reports 2008, p. 727.
16 Cf. The Danish Weekly Law Reports 2011, p. 2343.
17 Cf. The Danish Weekly Law Reports 2005, p. 1639.

Question 13

Under Danish law, there is in general broad access to be represented by others, and article 80 GDPR is not considered having any limiting effect on this access. Hence, no new legislative actions have been taken pursuant to article 80. So far, NGO's and other alternative movements play no significant role in the data protection enforcement in Denmark.

Question 14

At the moment there is no tendency for other regulators besides Datatilsynet to intervene in data processing related complaints. But Datatilsynet obviously cooperates with other relevant authorities, e.g. the Consumer Ombudsman and the Competition and Consumer Authority.

D Data Processing for National Security Purposes

Question 15

The notion of "national security" is not defined in either the Data Protection Act or the national act transposing the Law Enforcement Directive (Act no. 410 of 27 April 2017 on law enforcement authorities' processing of personal data).

Following the Court of Justice of the European Union (hereinafter "CJEU") its judgment in *Tele2/Watson*, the Danish Government has in principle accepted the application of the Charter to data retention for national security purposes.[18] However, like other EU Member States, Denmark is still considering exactly what consequences the judgment shall have for the Danish data retention rules.[19] Hence, the judgment has not yet led to any changes to the data retention rules.

The CJEU's judgment in *Tele2/Watson* has been applied by the Danish Eastern High Court in a recent case, where a group of copyright holders requested to obtain information from a telecommunications company about the name and address of IP addresses that had been used to download illegal material from the Internet.[20] However, the request was rejected. The court found, with reference to the relevant EU law and *Tele2/Watson*, that

18 Judgment of 21 December 2016 in C-203/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Tele2/Watson),* ECLI:EU:C:2016:970; See for more detail: S. Jakobsen, H. Udsen & A. Møller Pedersen, 'Data Retention in Europe – the Tele2 case and beyond', *International Data Privacy Law*, Vol. 8, No. 2, 2018, pp. 160-174.

19 Case C-203/15, *Tele2/Watson;* Which are found in Executive Order no 988 of 26 September 2006.

20 The Danish Weekly Law Reports 2019, p. 2019.

the protection of the personal data of the persons concerned exceeded the interest of the rightsholder's interest in obtaining the information.[21]

21 Case C-203/15, *Tele2/Watson.*

Estonia

Merike Kaev[*]

A Setting the Scene

Question 1

In Estonia, the General Data Protection Regulation (hereinafter "GDPR") is implemented in two ways:[1]

1. the Personal Data Protection Act[2]
   and
2. sector specific laws.

A The Personal Data Protection Act regulates:

1. protection of natural persons upon processing of personal data to the extent it elaborates and supplements the provisions contained in the GDPR;
2. transposition of Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data;[3]
3. the procedure for exercise of state supervision over compliance with the requirements for the processing of personal data;
4. liability for the violation of the requirements for processing of personal data.

---

* CIPP/E (Certified Information Privacy Professional/Europe), CIPM (Certified Information Privacy Manager), Data Protection Officer.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Personal Data Protection Act, https://www.riigiteataja.ee/en/eli/523012019001/consolide. All webpages referred to were last visited 9 February 2020.

3 Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

Specifications for application of the GDPR in the Personal Data Protection Act:

1. Processing of personal data for journalistic purposes;
2. Processing of personal data for academic, artistic and literary expression;
3. Processing of personal data for needs of scientific and historical research and official statistics;
4. Processing of personal data for archiving in public interest.

Other cases of processing personal data stipulated in the Personal Data Protection Act:

1. Processing of the personal data of children for the provision of information society services – minimum age requirement is 13;
2. Processing of personal data after the death of a data subject;
3. Processing of personal data in connection with violation of an obligation;
4. Processing of personal data in public places.

Overall, the Personal Data Protection Act is more about the transposition of Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, rather than implementation of the GDPR.

B Article 23 of the GDPR and sector specific laws:

1. The Personal Data Protection Act does not stipulate any restrictions based on article 23 GDPR;
2. Sector specific laws already in essence already entailed the types of restrictions set out in article 23 GDPR before the GDPR became applicable on 25 May 2018;
3. Sector specific laws were reviewed in light of the restrictions stipulated in article 23;
4. Approximately 113 sector specific laws were reviewed, and all other amendments, besides those related to article 23, were made. The focus on sector specific laws was intended to eliminate the main discrepancies with the GDPR, and not only those related to article 23.

National Supervisory Authority (hereinafter "NSA"):

In Estonia, there is one Supervisory Authority, the Estonian Data Protection Inspectorate, which oversees the enforcement of the GDPR, the Personal Data Protection Act and the provisions of sector specific laws that regulate personal data processing.

In addition to what is stipulated in article 57 GDPR, the Personal Data Protection Act regulates the competences and rights of the NSA, but these competences and rights are rather the reflection of article 57 GDPR than something relevantly new.

The office of the NSA has not significantly increased the number of its employees in light of the GDPR.

Question 2

Right to respect for private life and right to data protection:
The right to private life is regulated in § 26 of the Constitution of the Republic of Estonia (hereinafter "Constitution"), which stipulates that everyone is entitled to the inviolability of his or her private and family life.[4] Government agencies, local authorities, and their officials may not interfere with any person's private or family life, except in the cases and pursuant to a procedure provided by law to protect public health, public morality, public order or the rights and freedoms of others, to prevent a criminal offence, or to apprehend an offender.

Even though the Constitution does not regulate the right to data protection as an independent right, the commentary of the Constitution includes the right to data protection as an intrinsic part of one's privacy.[5] Sector specific laws regulate the right to data protection and personal data processing, that is, the rules that must be applied when someone wants to process personal data. Thus, the right to privacy is stipulated and regulated on the constitutional level, and the right to data protection is regulated on the lower level of legislation by general and sector specific laws. As the right to privacy is only regulated on the constitutional level, this right has been defined based on the example of the interpretation of article 8 of the European Convention on Human Rights. The GDPR, as a directly applicable EU regulation, is already by default a reflection of the Charter of Fundamental Rights of the European Union and its interpretation of the right to data protection, which all EU Member States must implement on a daily basis.

Court practice:
The Estonian Supreme Court – *Riigikohus* has a long-standing practice concerning the definition and scope of the right to privacy. In its decision 3-1-1-81-08, the Court explained that private life entails a person's entire private sphere, his or her entire way of life.[6] Thus, information about a person's place of residence, registered vehicles and committed offences can be considered part of his or her private life. In any case, the confidentiality of private information must be presumed where confidential information cannot be obtained by

4 The Constitution of the Republic of Estonia, §26, https://www.riigiteataja.ee/en/eli/521052015001/consolide.
5 Commentary on the Constitution of the Republic of Estonia. https://pohiseadus.ee/.
6 State vs J.P, Penti (Sup. Ct. 23 February 2009).

means other than through persons who have a statutory right to use confidential information for professional or occupational purposes.

Another decision by the Supreme Court that clarifies the scope of the right to privacy concerns the right to one's own image.[7] Here the Court has taken a firm view that the right to one's own image also belongs to the scope of §26 of the Constitution, in which the first sentence provides that everyone is entitled to the inviolability of his or her private and family life. Every person therefore has the right to decide how his or her image is used. In the opinion of the Court, a person's image can be used without the person's consent only to report on a current event involving the person. In addition, it is also required that use of the person's image is necessary for covering the current event and the public interest outweighs the person's interests. The defendant's action was illegal, as the defendant used the plaintiff's image without his consent and thus intruded unlawfully into the plaintiff's private life.

The interpretation of private life/privacy and data protection is still emerging and is only just finding its place compared to other areas of law, even though there was already quite a substantial amount of court practice under the old data protection regime.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Controllers have the right to decide the purposes for which personal data is processed, the type of data, on what legal ground, etc., as long as the GDPR requirements are fulfilled. The interpretation and application of GDPR principles as well as other parts of the GDPR may therefore vary depending on the area of business of the controller and the business interests involved. The GDPR also introduced a new principle, accountability, which obligates controllers to demonstrate that their processing activities are in accordance with the GDPR principles, which the controllers must prove with proper documentation. In general, this could mean that different controllers may interpret and apply GDPR principles differently, as long as they are able to prove that they have not violated the core essence of these principles. As the NSA's enforcement practice under the new data protection regime has been relatively, at the moment there is no clear understanding, at least on the part of the NSA, as to how adequately or appropriately controllers have interpreted and applied GDPR principles.

7 Tammeri vs TV3 AS (Sup. Ct.13 January 2010).

The domestic courts, foremost the Supreme Court, have made decisions regarding the legality of personal data processing under the old regime, based on Directive 95/46/EC, which was transposed into the Personal Data Protection Act.[8] The main questions have regarded the disclosure of personal data and accessibility of personal data. Many of these cases have related to the disclosure of personal data in the media or to a data subject who has requested access to his or her personal data in the framework of criminal proceedings or has requested access to his or her personal data that has been processed by public authorities.

In its interpretations regarding these principles, the Supreme Court has relied mainly on the case law of the European Court of Human Rights (hereinafter "ECtHR") as well as of the Court of Justice of the European Union (hereinafter "CJEU"). The broader practice of the domestic courts relating to data protection and privacy is still emerging.

The NSA has provided a general guideline on the GDPR covering a range of topics, but these principles have not yet been interpreted or applied by the NSA in practice. In its publications, the NSA has referred to the principles stated in the GDPR as being a natural part of all processing activity conducted by controllers, and hasn't added any additional explanations regards to principles.

Question 4

A recent decision by the Supreme Court on 6 June 2019 concerned the wrongful dismissal of a public official.[9] The official who had been dismissed from her position had experienced bullying at her workplace. To prove that she was being bullied, she recorded a conversation without asking the permission of the official whom she was recording. The Court concluded that when assessing the legitimate interest of the dismissed official, it was not relevant whether the personal data processing had helped achieve such legitimate interest. It is not possible to know this for sure at the time of processing personal data. In this case what was important was that personal data had been processed to achieve the legitimate interest, and the plaintiff had disclosed the recordings only to the Tax and Customs Board officials who had a decisive role in determining whether there had been bullying in the workplace. When defining an unspecified legal term such as "legitimate interest", it is first important to note that the controller's interest should be lawful for it to be achieved. It can also be concluded from article 7(f) of Directive 95/46/EC that the need for processing personal data should be real and not just hypothetical. The plaintiff had the overriding legitimate

8 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

9 Kingo vs Maksu- ja Tolliamet (Sup. Ct. 6 June 2019).

interest to get evidence of the alleged bullying in the workplace in order to demand that it be stopped.

This decision can be considered as the most detailed analysis of legitimate interest as a legal ground for processing personal data by the Estonian courts. In other decisions made by the courts regarding legitimate interest, of which there have been a limited number, the courts have mostly referred to the case law of the CJEU.

The Estonian courts have not interpreted consent as the legal ground differently or in more detail than the CJEU or ECtHR.

Question 5

There has not been any debate or decisions regarding this topic specifically, if at all. The issue itself has been tied to other topics relating to personal data and its processing. In recent years, the main debates have been about the GDPR specifically and what it states. The need to address abuse of personal data as "counter performance" is the subtext of the GDPR, but this has not yet been recognised in the national debate. Other EU level legal acts and different EU authorities have discussed this issue as one of the key issues relating to the digital single market.

Question 6

The Personal Data Act does not only implement the GDPR based on the discretion provided to the Member States, it also transposes the law enforcement directive, Directive (EU) 2016/680. In relation to implementation of the GDPR, the Act does not introduce any additional measures for ensuring this right, but it does reflect this right with regard to law enforcement, as provided for in the directive, which is transposed into national law through the Personal Data Act.

Question 7

In 2014, in case 3-3-1-97-08, the Supreme Court decided to satisfy the request of the petitioner to replace the petitioner's name with initials.[10] This right derives from the Code of Administrative Court Procedure. In this decision, the Court stated that it had not published the person's name in the Google search engine, and that the Court cannot replace the person's name with initials in the search engine.

10 M.O. application for deletion (Sup.Ct. 7 February 2014).

Overall, there has been little practice relating to the right to erasure, which has not received great attention by the courts or the NSA in Estonia so far.

Question 8

The Personal Data Protection Act states that personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, in particular if there is public interest and this is done in accordance with the principles of journalism ethics. Disclosure of personal data must not cause excessive damage to the rights of any data subjects. This is a general norm which is the foundation for processing for journalistic purposes. The same Act states that personal data may be processed without the consent of the data subject for the purpose of academic, artistic and literary expression, in particular if this does not cause excessive damage to the rights of the data subject. The same logic applies here as does in the case of journalistic purposes. There is no specific law that details how and under what circumstances personal data processing is allowed for these purposes. It is left to the courts and legal practice to develop the appropriate practice.

C Domestic Enforcement of Data Protection Law

Question 9

Under the GDPR, there is only one relevant public authority, that is, the Estonian Data Protection Inspectorate.[11] The Personal Data Protection Act regulates the qualifications required for appointment as head of the Estonian Data Protection Inspectorate. The Statute of the Inspectorate states the rights, obligations and responsibilities of the head of the Inspectorate, the number of staff of the Inspectorate and that the staff is to be appointed by a decree of the head of the Inspectorate.

In addition to what is stated already under point 1, the Personal Data Protection Act stipulates that in order to exercise state supervision provided for in the Personal Data Protection Act, the Estonian Data Protection Inspectorate may apply the specific state supervision measures provided for in §§ 30-32, 44, 49-53 of the Law Enforcement Act on the basis of and pursuant to the procedure provided for in the Law Enforcement Act.[12]

11 Estonian Data Protection Inspectorate, https://www.aki.ee/en.

12 Law Enforcement Act, https://www.riigiteataja.ee/en/eli/525032019010/consolide.

The NSA's contact details as well as the staff of the NSA are public information. The NSA currently employs 17 people, which also includes the head of the NSA, while two positions have not yet been filled.

To date, the NSA does not have a notable enforcement record under the GDPR, but they have executed some powers which fall under the scope of corrective and advisory powers.

Question 10

There is currently no specific strategy in place, or at least it has not been published. The Personal Data Protection Act states:

1. The Estonian Data Protection Inspectorate shall settle a complaint within 30 days after the date of filing the complaint with the Estonian Data Protection Inspectorate.
2. The Estonian Data Protection Inspectorate may extend the term for review of a complaint by up to 60 days in order to additionally clarify circumstances relevant to the settling of the complaint. The person who filed the complaint shall be notified of extension of the term in writing.
3. If co-operation with other relevant supervisory authorities is necessary for settlement of a complaint, review of the complaint shall be extended by a reasonable time period which is necessary to hear the other co-operating supervisory authorities or for them to state their opinion.

Question 11

No sanctions have been applied, although the NSA has in a couple of cases exercised powers which fall under the scope of corrective and advisory powers. Additional sanctions and/or additional measures that have been put in place to exercise supervision are described under Points 1 and 9.

Question 12

The Supreme Court in its decision 2-15-16007 stated that in the case of intangible harm, the court will determine fair compensation considering all the circumstances of the case.[13] Intangible harm entails foremost the physical and emotional pain and suffering of the person harmed. Damages for intangible harm are calculated based on the severity and the

13 Kulla vs Ekspress Meedia AS (Sup. Ct. 4 October 2017).

scope of the harm caused and also the behaviour and attitude of the person at fault towards the person who has suffered harm as a result of the violation. As there is no possibility to prove the exact amount of intangible harm, for the compensation of intangible harm it generally suffices to prove the circumstances which the law requires must exist for there to be a claim of intangible harm. The unlawfulness of the behaviour of the defendant is determined through weighing. The compensation for intangible harm is decided by the court based on its discretion. This specific case was also referred to the ECHR[14].

In the same decision, the Court referred to its previous decision[15] where it stipulated that when a person's privacy rights are being violated through the illegal disclosure of personal data, then for determining the amount of the sum of compensation, first the scope of the violation (for example, if the article was only published on paper or additionally online where presumably it will reach a significantly larger audience) must be taken into consideration. Other peculiarities of press offences (for example, the need to protect people from the forced commercialization of their lives) must also be considered. All circumstances which could influence the determination of fair compensation in the court case must be taken into consideration. In this case, the lower court awarded a total of 5000 euros for intangible harm, which the Supreme Court confirmed.

Overall, this is the logic applied in determining compensation in intangible harm cases, and most of these cases revolve around personal data disclosure in the media, commentating/defamation online, etc.

Question 13

No legislative measures have been introduced for facilitating such representative actions. At national level, there is one foundation, *Eesti Isikuandmete Kaitse* (Protection of Personal Data of Estonia), and also one NGO, *Eesti Andmekaitse Liit* (Estonian Data Protection Union). The activities of these organisations so far have been modest and are still evolving and finding their role within the new data protection regime.

Question 14

In Estonia, being a small country, it is normal practice for regulators of different areas to cooperate both formally and informally. There is no official mandate for cooperation between these regulators, or at least nothing has been published.

14 *Delfi AS v. Estonia* [GC], ECHR (2015), app. no. 64569/09, para. 34.
15 Plaintiff I, Plaintiff II vs Defendant (Sup. Ct. 26 June 2013).

D Data Processing for National Security Purposes

Question 15

"National security" is not defined in domestic law. There have been no major changes relating to data retention for national security purposes nor has this been specified in a somewhat more clear and detailed manner. It is more based on a case by case assessment.

The Supreme Court has stated that the invalidity of the directive does not inevitably cause the invalidity of the national rules, considering the goals of the directive.[16] The Member States have a certain level of discretion when adopting the national regulation. The collection, retention and use of communication data in criminal proceedings infringe the right to privacy. The Constitution allows for the restriction of this fundamental right in the cases provided for by law and in the interests of health, morality, public order or for the protection of other people's rights and freedoms, or the prevention of crime or apprehension of a criminal. The Supreme Court has found that requesting data from an internet service provider in relation to a criminal case corresponds to the purpose of § 26 of the Constitution in the sense of preventing a crime or apprehending a criminal. This measure is undoubtedly appropriate for guaranteeing these objectives. After the CJEU's decision in the Tele 2/Wat case, Estonia did not repeal the national law which transposed the EU directive.[17]

In 2018, the Supreme Court requested a preliminary ruling from the CJEU on the following questions:

1. Is article 15(1) of Directive 2002/58/EC(1) of the European Parliament and of the Council of 12 July 2002, in conjunction with articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union, to be interpreted as meaning that in criminal proceedings the access of State authorities to data making it possible to establish the start and end point, the date, the time and the duration, the type of communications service, the terminal used and the location of use of a mobile terminal in relation to a telephone or mobile telephone communication of a suspect constitutes so serious an interference with the fundamental rights enshrined in those articles of the Charter that that access in the area of prevention, investigation, detection and prosecution of criminal offences must be restricted to the fighting of serious crime, regardless of the period to which the retained data to which the State authorities have access relate?

16 R.V., J.L., T.S. and R.F. vs State (Sup.Ct. 23 February 2015).

17 Judgment of 21 December 2016 in Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970.

2. Is article 15(1) of Directive 2002/58/EC, on the basis of the principle of proportionality expressed in the judgment of the Court of Justice of 2 October 2018 in Case C-207/16, paragraphs 55 to 57, to be interpreted as meaning that, if the amount of data mentioned in the first question, to which the State authorities have access, is not large (both in terms of the type of data and in terms of its temporal extent), the associated interference with fundamental rights is justified by the objective of prevention, investigation, detection and prosecution of criminal offences generally, and that the greater the amount of data to which the State authorities have access, the more serious the criminal offences which are intended to be fought by the interference must be?
3. Does the requirement mentioned in the judgment of the Court of Justice of 21 December 2016 in Joined Cases C-203/ 15 and C-698/15, second point of the operative part, that the data access of the competent State authorities must be subject to prior review by a court or an independent administrative authority mean that article 15(1) of Directive 2002/58/EC must be interpreted as meaning that the public prosecutor's office which directs the pre-trial procedure, with it being obliged by law to act independently and only being bound by the law, and ascertains the circumstances both incriminating and exonerating the accused in the pre-trial procedure, but later represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative authority?[18]

18 H.K. vs State (Sup.Ct. 12 November 2018).

Finland

Anu Talus and Tobias Bräutigam[*]

A Setting the Scene

Question 1

The General Data Protection Regulation (hereinafter "GDPR") has been implemented in Finland mainly through the new Data Protection Act (1050/2018), which has been in force since 1 January 2019.[1] The Data Protection Act follows the structure of the GDPR. The new law includes provisions on the legal basis for processing, the supervisory authority and provisions regarding specific data or processing. According to the preparatory works, the Finnish Government has chosen to use many of the exemptions and opening clauses in order to be able to preserve the current legal situation. This concerns in particular the rules regarding the insurance sector and freedom of speech.

According to the Government Proposal, there was a special need to ensure that insurance providers would continue to have the right to process data in order to investigate insurance claims.[2] Given that this often includes the processing of sensitive personal data, the Finnish legislator wanted to ensure that there continues to be a legal basis for the processing. Consequently, § 6(1)(1) of the Data Protection Act uses the opening clause in article 9(1)(g) GDPR to allow the processing of health data outside of the rules for processing sensitive data. Insurance providers may process personal data related to criminal convictions and offences, as § 7 of the Data Protection Act points to § 6 of the Data Protection Act. Also teleoperators are entitled to process criminal records under certain circumstances, which is regulated in a separate act.[3]

---

* Anu Talus is currently Deputy Data Protection Ombudsman at the Data Protection Ombudsman's Office (Finland). At the time of drafting the report she held a post at the Ministry of Justice as senior legal adviser. Dr. Tobias Bräutigam is Senior Counsel at Bird & Bird, Helsinki (Finland).

1 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39; Tietosuojalaki ("Data Protection Act"), 1050/2018, in force since 1 January 2019.

2 HE 9/2018 vp, Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (hereinafter "Government Proposal"), p. 85 for further information on the legal basis.

3 Laki sähköisen viestinnän palveluista 145 §, 917/2014, in force since 1 January 2015 ("Electronic Communications Services Act").

Finland set the age limit for consent relating to the offering of information society services to 13 years, which is in line with other Nordic countries. The Government Proposal explains that the reasoning for having a lower age limit than the standard age limit of 16 years, set out in the GDPR, is that 13-year-olds are generally already used to using information society services and that these services are an important platform for self-expression and are also utilised for school work.[4] It was also brought up by supporters of a lower age limit that a higher age limit would simply lead to children circumventing the higher age restriction by lying about their age.

Another set of changes introduced by the Data Protection Act concerns the system of enforcement. The legislator thought it necessary to subject violations of article 10 GDPR to fines, as article 10 is not explicitly mentioned in the catalogue of provisions of article 83 GDPR.[5] The scope of article 83 has been extended to cover the abovementioned breaches. The Criminal Code has also been amended in connection with the implementation of the GDPR. More precise provisions regarding specific situations of wrongful use of personal data have been added to the Criminal Code. In particular § 9 of Chapter 38 of the Criminal Code was replaced with a new provision, which is narrower in scope than the previous provision. The new provision is titled Data Security Crime and it provides that criminal sanctions are only applicable in cases where the illegal processing of personal data is not within the scope of application of administrative fines provided by the GDPR. As the scope of those GDPR fines is rather wide, there is limited room for criminal sanctions.[6]

The degree to which the legislator protected freedom of speech in the Data Protection Act is especially interesting. In order to safeguard freedom of speech and the exchange of information, the application of several provisions of the GDPR has been excluded with regards purely journalistic purposes and the purposes of academic, artistic and literary expression. This issue will be further addressed under Question 8.

Many other acts and provisions have also been changed in connection with the implementation of the GDPR. These include acts on criminal matters and national security matters, law enforcement as well as social and health care.[7]

The Finnish Data Protection Ombudsman is the supervisory authority and shall oversee the application of the GDRP and the Data Protection Act in Finland. The Data Protection Ombudsman is supported by two Data Protection Deputy Ombudsmen and a board of five data protection experts. The Ombudsman may only issue fines jointly with the two

4 Government Proposal HE 9/2018 vp, p. 53.

5 Government Proposal HE 9/2918 vp, p. 10.

6 See, for example, art. 82(4)(a) GDPR, which includes a sanction for violations of art. 32 GDPR, the security of processing.

7 See e.g. HaVM 13/2018 vp, Hallintovaliokunnan mietintö, for a full list of the amendments www.eduskunta.fi/FI/vaski/Mietinto/Sivut/HaVM_13+2018.aspx. All webpages referred to were visited 21 August 2019.

Deputy Ombudsmen. The group of the Data Protection Ombudsman and the two Deputies is called *seuraamuskollegio*, sanction committee.

The Data Protection Ombudsman is also the supervisory authority for the Act on Processing of Personal Data in Criminal Matters and National Security Matters and has increased staff significantly over the years leading up to the GDPR.

Question 2

As a member of the European Union, Finland also follows the conceptual separation between data protection and privacy made by important international human rights instruments such as the Charter. The concepts are seen as different, albeit overlapping.[8] The Finnish Constitution provides in Chapter 2 Section 10 "the right to privacy" which states that "Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act." There is no separate constitutional protection for data protection, but Chapter 2 Section 10 is generally seen as also covering the right to data protection; especially in the preparation of new legal acts with an impact on data protection, the Constitutional Committee frequently mentions Section 10 as the bases for the constitutional guarantee of data protection.[9]

In legal practice, the difference is often not made explicitly. For example in a recent case dealing with the right to be forgotten, the court quoted both data protection and privacy, quite similar to the practice of the Court of Justice of the European Union (hereinafter "CJEU").[10] Finland follows the case law of the CJEU on data protection closely.

8 P.Korpisaari et al, *Uusi tietosuoja-lainsäädäntö*, Helsinki, Alma Talent, 2018, p. 14.

9 Compare pars pro toto the statement of 9 May 2019 by the Constitutional Committee concerning the Finnish Data Protection Act, which in its reasoning refers both to privacy and data protection as fundamental rights engrained in Section 10 of the Finnish Constitution: Perustuslakivaliokunnan lausunto ("The Constitutional Committee's Opinion") PeVL 14/2018 vp: www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_14+2018.aspx.

10 KHO:2018:112, 17 August 2018, www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1534308651626.html.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Traditionally the purpose limitation principle has been upheld in Finland in line with other European countries. Fair processing as a concept is little talked about and interpreted as linked to other principles of data protection, such as lawfulness, data subjects rights, data minimization and purpose limitation.[11]

The Finnish Data Protection Ombudsman has recently published a decision (2278/452/17) related to the credit information company Svea Ekonomi, where the processing was considered not to be lawful and fair.[12] According to the decision, the way the credit scores were established was discriminating as a too low or high age would cause an application for credit to be automatically inadmissible. As the activities were illegal, personal data processing connected to activities could not be considered to fulfil the requirements of lawful and fair processing. It is worth noting that the decision was not only based on article 5(1) GDPR, but also on the Credit Information Act (luottotietolaki).[13]

Question 4

So far, there has not been any interpretation by Finnish courts on the concepts of consent or legitimate interest. Legitimate interests as a legal basis was not included as such in the Personal Data Act, which preceded the Data Protection Act in Finland. There was a more specific provision in the Act that allowed processing of personal data based on a customer or service relationship.[14] Many cases that currently fall under the legal basis of legitimate interest could be covered by this provision. When there was a need for legitimate interests generally as a legal basis, practitioners either applied Directive 95/46 directly, based on the CJEU judgment in *ASNEF* or asked the so called Data Protection Board for approval.[15]

---

11 The leading Finnish commentary on the GDPR includes only a few lines on the principle of fairness, whereas other principles in art. 5 receive more attention, compare Korpisaari & Pitkänen & Warma-Lehtinen, 2018, p. 90.

12 Tietosuojavaltuutetun päätös rekisteröidyn oikeuksien toteuttamisesta, 15 February 2019, Drn 2278/17, pp. 6-7.

13 Luottotietolaki ("Credit Information Act"), 527/2007, in force since 1 November 2007. According to art. 33 of that law, the Data Protection Ombudsman is the supervising authority for this law concerning the exchange of credit information.

14 Personal Data Act ("Henkilötietolaki") 8 § (5), 1999/523, was applicable 01.06.1999 – 31.12.2018.

15 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31; judgment of 24 November 2011 in Joined Cases C-468/10 and C-469/10, *Asociación Nacional*

The Data Protection Board elaborated the notion of legitimate interests when issuing permits. With the new Data Protection Act, the Data Protection Board has been abolished. It is too early to say how the concept of legitimate interests in data processing will develop in Finland.

Question 5

There have so far been no decisions in Finland regarding the problem of the validity of the business model of free digital content in return for personal data. In general, Finnish media companies do not collect the same amount of personal data for personalization as international social networks would do in their 'counter-performance' models.

The Finnish Competition and Consumer Authority has warned consumers about the value of data.[16] The issue of data as payment falls under the competence of both the Finnish Competition and Consumer Authority and the Finnish Data Protection Ombudsman. The latter did not address the issue specifically in its guidance on fairness of processing.[17]

Question 6

The Finnish legislator has chosen to limit the right not to be subjected to automated decision-making, including profiling, under narrow circumstances. Data subjects may not invoke this right in the event that personal data is processed for purely journalistic purposes or for the purposes of academic, artistic or literary expression. This limitation of the right was introduced to safeguard freedom of speech and freedom of expression, which are protected under the Finnish Constitution.[18] While the legal basis for the exemptions lie in article 85 GDPR, not in article 22(2)(b), the effect is the same.

Question 7

Search engines in Finland operate under the same terms as in other EU countries.[19] In the first years after the *Google Spain* decision, the Data Protection Ombudsman exercised a

---

de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, ECLI:EU:C:2011:777, para. 52.

16 Kilpailu- ja kuluttajavirasto ("Finnish Competition and Consumer Authority"), www.kkv.fi/ajankohtaista/Uutiset/2019/28.2.2019-kuluttajavinkki/.

17 Tietosuojavaltuutetun toimisto ("Office of the Data Protection Ombudsman"), tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys.

18 Perustuslaki ("Finnish Constitution") 12 §, 731/1999, in force since 1 March 2000.

19 The instructions on Google's page on "Personal Information Removal" are a close translation from the English text. The page is accessible at: policies.google.com/privacy?hl=fi&gl=fi#infodelete.

certain restraint regarding complaints concerning the right to be delisted.[20] In one prominent case, the Ombudsman stated that there was no need to delete the search results leading to a business register list because the person in question was still being involved in business operations, including debt collection.[21]

In a more recent case, the Data Protection Ombudsman had requested Google to remove links leading to websites that contained information on a murderer's health condition. The Ombudsman prevailed before the Supreme Administrative Court.[22] In this case, the applicant had been sentenced to prison for murder. He had been found criminally responsible to a lower degree as he had Asperger syndrome. Persons typing the applicant's name in Google's search engine were easily led to several search results in which the applicant's name, his medical condition and his criminal sentence were discussed. The applicant made a request to the Data Protection Authority to have the Google search results removed. The Ombudsman then made a request to Google for removing the links to that data, but Google denied this request. Google stated that it was in the public interest to keep the information available to the public as there were strong legitimate interest grounds to inform people of the applicant's crimes for the protection of public safety.

The Ombudsman held that the data concerning the medical condition of the applicant was not relevant information in the light of the Personal Data Act (the predecessor of the current Data Protection Act) and therefore must be erased. The right to privacy of the applicant overrode the public interest grounds that Google invoked. The first instance administrative court sided with the Data Protection Authority's reasoning and the Supreme Administrative Court upheld the decision of the administrative court.

Question 8

As stated in the context of question 6, the Finnish legislator has decided to exclude many provisions of the GDPR in favour of freedom of expression. This concerns the processing of personal data for the purposes of journalistic, academic, artistic and literary expression.[23] The application of the following provisions of the GDPR has been excluded in this context: article 5(1)(c-e), article 6, 7, 9 and 10, article 11(2), article 12-22, article 30, article 34(1-3), articles 35-36, article 56, article 58(2)(f), articles 60-63 and article 65-67. Especially the exclusions on the rights of individuals are wider than in many Member States.

---

20 Judgment of 13 May 2014, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

21 Yle-article, *Google wins first "right to be forgotten" case in Finland*, 12 May 2015, https://yle.fi/uutiset/osasto/news/google_wins_first_right_to_be_forgotten_case_in_finland/7988957.

22 KHO:2018:112 (17 August 2018).

23 Government Proposal HE 9/2018, pp. 107-113; Tietosuojalaki ("Data Protection Act") 27 §, 1050/2018, in force since 1 January 2019.

This approach has mainly been justified by reference to the status quo, i.e. the previous Personal Data Act, and the goal to maintain a similar level of protection for freedom of speech. Both the Finnish Act on Freedom of Speech and the Criminal Code include safeguards for data subjects that are considered to balance out the exemptions made to the application of the GDPR.

The Government Proposal recognizes the conflict between freedom of speech and data protection and points to the *Satamedia* case as an example of how two fundamental rights can be balanced.[24] In this case,[25] the Court of Justice had to balance freedom of expression versus data protection as fundamental rights and decided that limitations and exceptions to the right to privacy had to be applied only in so far as strictly necessary. This balancing approach is present in the Government Proposal, and Section 27 of the Finnish Data Protection Act leaves it also in the future for the courts' interpretation.[26]

The wide exemptions to data protection rights and obligations date back to the previous Personal Data Act. In the working group of the Ministry of Justice, the goal to preserve the status quo was stressed.[27] Certain rights are also safeguarded through provisions in the Criminal Code and the Act on Freedom of Speech, such as the right to rectify incorrect information.

According to the Government Proposal, the regulatory situation between the different rights had been well balanced.[28] This was the case partly due to the efficient self-regulatory system for journalism in place in Finland.[29] It remains to be seen how the courts will interpret the vast restriction of data subject rights, including article 22 GDPR. In the past, the Supreme Administrative Court took security measures into account to uphold data subjects' rights.[30] In any case, the provisions in the Data Protection Act restricting Data subject rights need to be interpreted in light of the Charter of Fundamental Rights of the European Union (hereinafter "Charter") and the European Convention on Human Rights.

---

24 Government Proposal HE 9/2018 vp, p. 46.

25 Judgment of 16 December 2008 in Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,* ECLI:EU:C:2008:727.

26 Tietosuojalaki 27 §, 1050/2018.

27 EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän mietintö, mietintöjä ja lausuntoja ("Ministry of Justice working group paper on the implementation of the GDPR") 35/2017, p. 65, julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf.

28 Government Proposal HE 9/2018 vp, p. 47 and p. 126.

29 Government Proposal HE 9/2018 vp, p. 47.

30 KHO:2015:44, 27 March 2015, www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1427281003635.html.

C Domestic Enforcement of Data Protection Law

Question 9

The Finnish Data Protection Act sets down the office of the Finnish Data Protection Ombudsman.[31] The Data Protection Ombudsman supervises the application of the GDPR and the Law Enforcement Directive (hereinafter "LED"). The supervision of the Credit Information Act falls also under the Data Protection Ombudsman's remit.[32] The scope of this law covers more widely data related to credit information, including information related to corporations and companies. Furthermore, sector specific legislation drawing from the national margin to manoeuvre provided by the GDPR falls under the Data Protection Ombudsman's remit.

The Data Protection Ombudsman's office builds on the institutional structure which was in place under the previous data protection regime. The head of office is the Data Protection Ombudsman as before. However, some significant changes were introduced with the adoption of the Finnish Data Protection Act. For example, the Data Protection Ombudsman institution was strengthened with two Deputy Data Protection Ombudsmen.

The Data Protection Act also reformed institutional structures of the enforcement mechanism. Under the previous data protection regime, a Data Protection Board existed parallel with the Data Protection Ombudsman. The Data Protection Board had some enforcement powers and it also had a competence to issue permits for the controllers. This Board was abolished with the new Data Protection Act.[33] Instead a new Expert Board was introduced with the Data Protection Act. The Expert Board consists of a chair, vice-chair and three members.[34] The government appoints the Expert Board for a term of three years. The role of the Expert Board differs significantly from the previous Data Protection Board.[35] Where the Data Protection Board had the competence to issue binding decisions based on Data Protection Ombudsman's application, the Expert Board's role is limited in giving opinions upon a request by the Data Protection Ombudsman. The Data Protection Act limits the Expert Board's tasks to high profile issues related to application of the data protection legislation.[36] The opinions issued by the Board are not binding, but they can provide very valuable insight in complex cases. The Expert Board as is the case with the Data Protection Ombudsman is allowed to hear and use external experts.[37]

31 Tietosuojalaki 8 §, 1050/2018.
32 Luottotietolaki 33 §, 527/2007.
33 Tietosuojalaki 37 §, 38 § (1), 1050/2018.
34 Tietosuojalaki 12 § (1), 1050/2018.
35 Tietosuojalaki 12 §, 1050/2018.
36 Tietosuojalaki 17 § (1), 1050/2018.
37 Tietosuojalaki 17 § (2), 19 §, 1050/2018.

The Data Protection Ombudsman is independent in its decision making and solves the cases based on presentation of one its staff members. Similarly, the Deputy Data Protection Ombudsmen make decisions independently based on presentation. The three Ombudsmen can exercise certain powers only as a collegium. This is the case regarding issuing administrative fines. The three Data Protection Ombudsmen form a collegium and the collegium makes it decisions based on presentation by a staff member. In case the collegium votes, position of majority prevails. If the votes are divided evenly, the less heavy sanction prevails.[38]

The collegium composition, or more precisely any composition involving multi-member formation, was required by the Constitutional Committee during the parliamentary process. The Constitutional Committee underlined that significant public powers are applied when administrative fines are issued; the constitutional committee saw it therefore essential that the decision making takes place in broader formation and not in a one-person composition.[39]

The Data Protection Ombudsman and the Deputies are all selected and appointed in a similar manner. Also, on more general terms, the same requirements apply for the Data Protection Ombudsman and the Deputies.[40] Furthermore, all Data Protection Ombudsmen have the same enforcement powers.[41] The Data Protection Act specifies the qualification requirements for the Data Protection Ombudsman. The Data Protection Ombudsman must have a higher legal degree, good knowledge in data protection issues and management experience. Also the skills to deal with international issues was seen necessary requirement for the Data Protection Ombudsman due to the increasing role of the European decision making body and international dimension of the data protection issues.

The government appoints the Data Protection Ombudsman for a five-year term.[42] This term is renewable.[43] The opening of the position is first published.[44] Also the information of the candidates is publicly available as a rule. The decision of the appointment is available on the government's website and the memorandum reasoning the appointment is provided for anyone by a request. The non-chosen applicants can appeal the decision to Administrative Court if they so wish.[45] The First Deputy Data Protection Ombudsmen

38 Tietosuojalaki 24 § (2), 1050/2018.

39 PeVL 14/2018 vp; PeVL 24/2018 vp.

40 Unless otherwise indicated, what is said of the Data Protection Ombudsman in this writing applies to the Deputies as well.

41 Unless precisely otherwise indicated, what is said about the Data Protection Ombudsman applies also to the Deputy Ombudsmen.

42 Tietosuojalaki 11 § (1), 1050/2018.

43 See Government Proposal HE 9/2018 vp, p. 96. The Government Proposal clarifies that it follows from the Finnish legal order that the term is renewable unless otherwise specifically regulated.

44 Valtion virkamieslaki ("State Official Act") 5a §, 750/1994, in force since 1 December 1994 and regarding 35 § (1) since 1 January 1996.

45 Valtion virkamieslaki 59 §, 750/1994.

were appointed in the end of April 2019. There were 19 and 13 candidates for these posts, which had slightly different emphasis regarding the qualifications.

As for the recruitment of staff for the Data Protection Ombudsman's Office, the new Data Protection Act did not bring notable changes for the selection procedure. The most significant amendment relates to the appointment of the administrative head of office. When the administrative head of office (*toimistopäällikkö*) was previously appointed by the Ministry of Justice, all staff members are now appointed by the Data Protection Ombudsman, including the head of administration. Previously the head of administration acted also as the deputy for the Data Protection Ombudsman. This has now changed with the introduction of the Deputy Data Protection Ombudsman posts.

The Data Protection Ombudsman did select and appoint its staff also under the previous Data Protection Act. The Data Protection Ombudsman's office has now been strengthened with a significant number of new legal experts and other staff. The number of all employees including the Data Protection Ombudsman and the Deputies is currently 44. Also, the Data Protection Act itself underlines that the office shall have needed number of employees. As for the Deputy Data Protection Ombudsmen, the Data Protection Act sets only a minimum number for the deputies, which is two. However, there is an opening for more than two deputies if this will later seem necessary. The minimum number of deputies ensures that the data protection authority is always capable of using all of its powers, including issuing fines.[46]

Besides the powers and tasks endowed to the Data Protection Ombudsman by the GDPR and the LED, the Data Protection Ombudsman is provided with some additional tasks deriving from the sector legislation. The Data Protection Ombudsman for example supervises the application of the Credit Information Act (*luottotietolaki*). This might include issues related to data which is not personal data. The Data Protection Act also provides the Data Protection Ombudsman with certain powers, which complete the powers and tasks regulated in the GDPR. To ensure the proper functioning of the Data Protection Ombudsman, the Data Protection Ombudsman has the right to receive the information which is necessary for conducting his/her duties. Based on the national Data Protection Act, the Data Protection Ombudsman has for example the right to receive all information which is necessary to fulfil its duties. The Data Protection Act specifies that no costs can be demanded from the Data Protection Ombudsman when exercising this right. Furthermore, the Data Protection Ombudsman has the right to receive information regardless of the rules on classification.[47] The Data Protection Ombudsman has also the right to receive assistance from the police in order to fulfil its duties.[48]

46 As explained earlier, certain powers can be applied only in a formation of three.
47 Tietosuojalaki 18 § (1), 1050/2018.
48 Tietosuojalaki 20 §, 1050/2018.

Furthermore, the Data Protection Ombudsman has also the right to conduct a control visit at premises, if this is necessary in order to investigate the matter and there is a specified and reasoned ground to suspect that data protection provisions have been violated in a manner which falls under administrative fines or criminal penalties.

Furthermore, besides the duties following from the GDPR, the Finnish Data Protection Ombudsman accredits the certification body. This follows from article 14 § 4 mom. of the Data Protection Act.[49]

The Data Protection Ombudsman received 57 requests for statements from the prosecutors and courts in 2017 and 64 in 2018. It gave 51 statements in 2017 and 80 in 2018.

Question 10

The Data Protection Ombudsman's Office has not communicated a specific strategy for GDPR supervision.

The legislative framework does not set limits for the Data Protection Ombudsman to prioritize specific cases. Prioritizing could refer to allocation of resources or assessing how time-pressure influences the proceedings. The Data Protection Ombudsman strives to organize its work in the most effective manner. As an authority with statutory duties, the Ombudsman is not free to drop cases, i.e. all cases, including non-prioritized, are examined in due course.

In case data subjects are not satisfied with the treatment of their cases at the Data Protection Ombudsman Office, they can lodge a complaint with the Parliamentary Ombudsman or the Chancellor of Justice. Those institutions are the highest overseers of legality in Finland. The complaint could relate for example the length of the decision making.

Question 11

The Data Protection Act excluded the application of administrative fines on the public sector. This was reasoned for example by the specific liability civil servants are bind to when carrying out their duties. This restriction does not apply for conditional fines, which can be issued to the public sector as well. Conditional fines are issued together with the Data Protection Ombudsman's decision and in case the addressee of the decision does not comply with the decision, the conditional fines can be enforced on the addressee. In limited cases, the Data Protection Ombudsman and Data Protection Board had this power also

49 Tietosuojalaki 14 § (4), 1050/2018.

under the previous data protection regime.[50] It was used quite sparingly as the decisions made by these authorities were usually implemented by the controllers.

Question 12

It is possible to be awarded damages for intangible harm in Finland. However, this has not occurred in the data protection field under the previous regime. The Finnish system is generally speaking very restrictive in awarding damages for intangible harm. In other areas of law, it is not uncommon that courts award almost symbolic fines.

Question 13

The Finnish Data Protection Act did not introduce any new measures related to article 80 of the GDPR nor is there general legislation on this topic. However, the so-called TATTI working group, which did the preparatory work for the Data Protection Act did note, that article 80 provides the possibility of representative actions. The TATTI working group did conclude that there might be a need to seize the possibility provided by article 80. This would, however, require more comprehensive analysis and preparatory work. The working group did propose that the demand for providing the means for this type of actions would be examined later.[51]

In Finland, NGOs have not occupied a large space in the data protection discussion in comparison with some other Members States, like Austria or Germany. Instead the discussion has been dominated by public authorities, controller's representatives and when the focus is on the fundamental right dimension, academics. NGOs focusing data privacy and digital rights do exist in Finland and they are becoming increasingly involved in the public debate. For example, the Electronic Frontier Finland (Effi)[52] and the Open Knowledge Finland (OKFI)[53] have both contributed in the data protection discussion. During the legislative procedure all parties willing to contribute in the process can submit their statement on the draft law for the responsible ministry. The Ministry of Justice maintains a platform providing this possibility and both Effi and OKFI did submit their statements on the Finnish Data Protection draft law.[54] Also, for example the former Finnish Data

50 Henkilötietolaki 46 §, was applicable 01.06.1999 – 31.12.2018.

51 EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän mietintö, mietintöjä ja lausuntoja ("Ministry of Justice working group paper on the implementation of the GDPR") 35/2017, p. 63, julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf.

52 www.effi.org.

53 fi.okfn.org.

54 Ryhmäkannelaki, 444/2007, in force since 1 October 2007. For more information, see also: www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1d738195-b96a-47b8-8a74-6ddda342da60.

Protection Board, which had a role in the enforcement of data protection law, had a member with Effi-background.

Furthermore, sometimes data protection issues emerge in the consumer's rights in a manner, which leads into the involvement of consumer authorities. There are several public authorities in Finland representing the consumer interest; Competition and Consumer Authority[55], Consumer Advisory Services[56], Consumer Ombudsman[57] and Consumer Complaint Board[58], which solves issues related to consumer rights.

Consumer authorities have certain tools to address situations where similar issues occurs in multiple cases, these are group complaint and class action. The Consumer Ombudsman has the competence to initiate a group complaint on his/her own initiative. In such case the Consumer Ombudsman considers similar disputes as single matter. This does not require a request from the consumer. The Consumer Ombudsman has also competences to file a class action. Only the Consumer Ombudsman has this competence; these competences were endowed to the Consumer Ombudsman to further strengthen the group complaint. The members of the class must be individually defined and they must opt-in to participate in the class action. The class action matters fall under the jurisdiction of the district court of Helsinki.[59]

Question 14

The Data Protection Ombudsman has cooperated with other regulators, such as consumer authorities, already during the previous data protection regime.

The cooperation has continued after the GDPR became applicable. A recent example of cooperation between Data Protection Ombudsman's Office and consumer authorities dates from June 2019. The Data Protection Ombudsman addressed then jointly with the consumer authorities the general public on robocalls. Robocalls had recently caused confusion among consumers in Finland. Both the Data Protection Ombudsman and consumer authorities are examining a case, where robocalls had been used for direct marketing. The press release published on the Data Protection Ombudsman's website

55 www.kkv.fi/Tietoa-KKVsta/.
56 www.kkv.fi/en/consumer-advice/.
57 www.kkv.fi/Tietoa-KKVsta/kuluttaja-asiamies/.
58 www.kuluttajariita.fi/fi/.
59 Finnish Competition and Consumer Authority, *Assisting the consumer in court-group complaint and class action,* 20 November 2014, www.kkv.fi/en/about-us/the-consumer-ombudsman/assistance-provided/.

clarifies to which authority consumer should turn to depending on the specific robocall issue at stake.[60]

D Data Processing for National Security Purposes

Question 15

The LED was implemented into Finnish legislation by *laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä* (1054/2018). This translates as an Act on the processing of personal data in criminal matters and in the context of maintaining national security. It was a national decision to extend the scope of the Act on implementing the LED to cover the processing of personal data when maintaining national security. It follows from the Finnish Constitution that all processing of personal data must be regulated by law. That includes processing for the purpose of national security. This Act does not, however, try to define the concept of national security.

This solution was not widely debated during the legislative process, but was rather seen as a reasonable solution. As the Act on implementing LED falls under the Data Protection Ombudsman's remit, the Ombudsman also supervises matters related to national security in so far as the said Act is applicable.

Another Act covering the intelligence services entered into force on 1 July 2019. This is of high relevance in the context of national security; it also includes location data, i.e. personal data in this context. One of the safeguards to assure appropriate functioning of intelligence services was setting up the institution of the "Intelligence Ombudsman". The new institution functions in the context of the Data Protection Ombudsman's office, but is a separate entity from the Data Protection Ombudsman.

60 The Data Protection Ombudsman, *Robots cannot make telephone sales calls without consumer's consent*, 14 June 2019, tietosuoja.fi/fi/artikkeli/-/asset_publisher/robotti-ei-saa-soittaa-myyntipuheluita-ilman-suostumusta?_101_INSTANCE_ajcbJYZLUABn_languageId=en_US.

France

Céline Castets-Renard, Mathieu Combet and Olivia Tambou[*]

A Présentation du contexte

Question 1

En France, les deux principaux textes adaptant le droit français au Règlement Général sur la Protection des Données (ci-après « RGPD ») et transposant la Directive Police Justice sont actuellement la nouvelle loi Informatique et Libertés (ci-après « LIL ») et le décret n°2019-536 du 29 mai 2019 entrés en vigueur le 1er juin 2019. La LIL comporte actuellement 128 articles répartis en cinq titres:

- Titre Ier: Dispositions communes, consacré notamment aux principes, définitions, à l'autorité de contrôle qui est la Commission Informatique et libertés (ci-après « CNIL »), formalités préalables, voies de recours,
- Titre II: Traitements relevant du RGPD
- Titre III: Dispositions applicables aux traitements de la directive Police Justice
- Titre IV: Dispositions applicables aux traitements intéressant la sûreté de l'Etat et la défense;
- Titre V: Dispositions relatives à l'outre-mer

Cette présentation ainsi que le "choix" d'opérer de nombreux renvois au RGPD en raison de son effet direct rend le texte final parfois peu lisible voire inintelligible pour des non spécialistes. En outre, on constate des phénomènes tantôt de sur-adaptation visant à aller au-delà des règles ayant effet direct du RGPD, tantôt de sous-adaptation visant à maintenir des règles nationales antérieures dont la formulation n'est pas conforme à celle du RGPD.[1]

D'une manière générale, le gouvernement a estimé que le RGPD comportait une liste de 56 renvois au droit national. Il a été décidé de faire une utilisation modérée des marges d'appréciation[2] laissées aux Etats membres par le RGPD. Une part importante de l'usage

---

* Les questions 3,5,6,10, 11 ont été préparées par Céline Castets-Renard, Full Professor à l'Université d'Ottawa, les questions 2,4,7,12 et 14 par Mathieu Combet Maître de Conférences à l'Université de Saint-Etienne, les questions 1,8,9,13, 15 par Olivia Tambou, Maître de Conférences à l'Université Paris-Dauphine.

1 C'est notamment le cas pour les règles relatives à l'article 80 RGPD cf. notre analyse question 13.

2 Pour plus de détails cf. notre article 'French Adaptation of the GDPR', *in* K. Mc Cullagh et al. (Eds), National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxembourg (2019), https://

des dérogations et limitations concerne les autorités publiques ou certaines catégories de traitements de données.

Les principales flexibilités au RGPD existant en France sont:

- **Une disposition relative au droit applicable en cas d'usage de clauses ouvertes par les Etats membres** Cette question n'a pas été abordée dans le RGPD. La France a néanmoins pris l'initiative de préciser que lorsque le RGPD renvoi au droit national le soin de l'adapter le droit français s'applique en principe "*lorsque la personne concernée réside en France y compris lorsque le responsable de traitement n'est pas établi en France*" (article 3, II LIL). Le critère de résidence est remplacé par le critère de l'établissement lorsque des traitements à des fins journalistiques ou à des fins d'expression universitaire, artistique, ou littéraire sont en cause. Autrement dit, le droit français s'appliquera, dès lors que le responsable du traitement est établi en France.
- **Les données post-mortem** (considérant 27 RGPD, articles 84-86). Exclues du champ d'application du RGPD, les données personnelles des personnes décédées font l'objet de dispositions introduites en France en 2016 par loi n° 2016-1321 dite République numérique. Il s'agit notamment de permettre aux personnes de laisser des directives relatives au traitement de leurs données personnelles après leur mort (testament numérique) et de préciser les droits pouvant être exercés par les héritiers en l'absence de ces directives.
- **L'interdiction des traitements des données sensibles** (article 9 RGPD, article 44 de la LIL).

  Six types de traitements de données sensibles sont possibles en France:

  1. Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel
  2. Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels
  3. Les traitements comportant des données concernant la santé justifiée par l'intérêt public
  4. Les traitements conformes aux règlements types mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires;

---

blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf. Toutes les pages Web ont été consultées pour la dernière fois le 5 février 2020.

5. Les traitements portant sur la réutilisation des informations publiques sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées;
6. Les traitements nécessaires à la recherche publique

- **L'âge du consentement du mineur (article 8 RGPD, article 45 de la LIL).** La France a opté pour une solution inédite qui prévoit:
  - avant 13 ans le consentement du seul titulaire de l'autorité parentale,
    a. entre 13 et 15 ans le consentement conjoint du mineur et du titulaire de l'autorité parentale. La conformité du double consentement a été justifiée tant par le gouvernement que par le Conseil constitutionnel français[3] par la lettre 8 RGPD qui distingue le consentement donné, du consentement autorisé. Pour autant, cette interprétation unilatérale du RGPD peut interroger
    b. Après 15 ans, le consentement du seul mineur.
- **Traitement des données à caractère personnel relatives aux condamnations pénales** (article 10 RGPD, article 46 LIL). Six catégories de personnes peuvent traiter ces données particulières. La principale nouveauté est d'avoir introduit "Les réutilisateurs des informations publiques … sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernée". Il s'agit de répondre à l'engagement politique de la France en matière d'Open Data.
- **Fondement légal pour des décisions administratives individuelles exclusivement automatisées** (article 22 RGPD §2b), article 47 de la LIL cf. réponse question 6 pour plus de détails)
- **Quelques limitations de droits** (article 23 RGPD, article 48, 49, 52, 58 LIL)
  a. **pas de droit à l'information pour les données collectées indirectement** (article 14 RGPD) pour certains traitements mis en œuvre pour le compte de l'Etat intéressant la sécurité publique, le contrôle et le recouvrement des impôts (article 48 LIL)
  b. **pas de droit d'accès** pour les traitements aux seules finalités d'établissement de statistiques ou de réalisation de recherche scientifique ou historiques et sous certaines conditions (article 49, alinéa 3 LIL).
  c. **droit d'accès, de rectification et d'effacement indirect** par le biais de la CNIL pour certains traitements liés au contrôle et recouvrement des impôts (article 52 LIL)
  d. pas **de communication à la personne concernée de violation de données** (article 34 RGPD, article 58 II LIL) pour une catégorie de traitements dont la communication serait susceptible d'engendrer un risque pour la sécurité nationale, la défense ou la sécurité publique**.** Liste des traitements concernés à l'article. 85 du décret n°2019-536.

3 cf. Point 63 de la décision du Conseil Constitutionnel nº 2018-765 du 12 juin 2018.

- **Des limitations de droits** découlant de l'article 85 RGPD cf. question 9.
- **Le maintien de quelques formalités préalables** (Chapitre IV de la LIL, articles 31-36): Une autorisation préalable a été maintenue pour:
  - des traitements de souveraineté, (article 31-1 LIL),
  - certains traitements dans le domaine de la santé (article 66 III LIL),
  - certains traitements de données génétiques ou biométriques (article 32 LIL).
- **Etablissement d'une liste limitative de personnes pouvant traiter le NIR** (numéro d'inscription au répertoire), article 30 LIL, décret n°2019-341 du 19 avril 2019.
- **Traitement des données dans le cadre des relations de travail (art. 88 du RGPD),** existence de règles en matière de vidéosurveillance, droit d'information du salarié, traitement des fiches de paie, dans le code du travail (notamment article L1221-9 et L-1222-4)
- **Prise en compte de certains publics: mineurs, TPE, PME, collectivités locales**
  - L'article 48 alinéa 2 de la LIL précise que l'information au titre de l'article 13 du RGPD doit être transmise au mineur de moins de 15 ans "*en langage clair et facilement accessible*".
  - Mission de la CNIL visant en accompagner plus particulièrement ces acteurs.

Question 2

En droit français, le droit au respect de la vie privée a été introduit à l'article 9 du Code civil, introduit par la loi du 17 juillet 1970. De son côté, la protection des données personnelles a été introduite par LIL en 1978 modifiée par la loi n°2004-801 du 6 août 2004 pour l'adapter à la directive 95/46 CE et enfin par la loi n°2018-493 du 20 juin 2018 pour l'adapter au RGPD et à la Directive Police Justice.

C'est en raison des risques d'atteintes à la vie privée des personnes que la protection des données personnelles a été intégrée au droit au respect de la vie privée. C'est ce qui ressort de certaines décisions du Conseil Constitutionnel comme la décision n°2012-652 du 22 mars 2012 sur la loi relative à la protection de l'identité sur le fondement de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

La Charte européenne sur les droits fondamentaux (article 8) a eu une influence sur la protection du droit à la protection des données qui n'était pas reconnue comme un droit fondamental en France. Au demeurant, le contentieux portant sur ces questions ne se fonde pas directement sur les dispositions de la Charte, mais sur des textes nationaux ou de droit dérivé. Il n'en demeure pas moins que la jurisprudence de la Cour de justice de l'Union européenne a eu une certaine influence sur la protection des données personnelles

comme avec le droit à l'oubli avec notamment l'arrêt *Google Spain* de 2014[4] ou bien encore l'arrêt *Manni* de 2017.[5]

Dans 13 arrêts rendus le 6 décembre 2019[6], le Conseil d'Etat s'est prononcé sur le droit au déréférencement en tirant les conséquence de l'arrêt de la Cour de justice le 24 septembre 2019 consacrant le champ européen et non mondial du « droit au déréférencement ».[7] Cela a été également le cas de la Cour de cassation dans un arrêt rendu le 27 novembre 2019.[8]

B Réception des dispositions de fond du RGPD dans l'ordre juridique national

Question 3

Il a été décidé de ne pas répondre à cette question afin de respecter la taille et en raison de l'absence d'éléments scientifiques pour y répondre.

Question 4

Le Conseil d'Etat a eu l'occasion de se prononcer sur la notion **"d'intérêt légitime"** dans un arrêt du 18 mars 2019 dans le cadre d'une procédure d'une personne exerçant son droit d'opposition à l'exploitation des données personnelles de ses enfants.[9]

Selon le Conseil d'Etat, le droit de toute personne physique de s'opposer au traitement de ses données personnelles, conformément à l'article 38 de la LIL est subordonné à l'existence de raisons légitimes. Ces dernières doivent tenir de manière prépondérante à la situation particulière du demandeur. C'est-à-dire que le fait de faire état de craintes d'ordre général sans pour autant évoquer des considérations qui sont propres à la situation de ses enfants n'est pas suffisant pour établir l'existence d'un motif légitime.

Si le Conseil d'Etat ne s'est pas prononcé sur le fondement du RGPD en raison du fait qu'il n'était pas applicable aux moments des faits, il est intéressant de noter que l'article 21 relatif au droit d'opposition prévoit, quant à lui, que « la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un

4 CJUE 13 mai 2014, *Google Spain SL, Google Inc. c/ Mario Costeja González* e.a., aff. C-131/12, ECLI:EU:C:2014:317.

5 CJUE 9 mars 2017, *Camera di Commercio c/ S. Manni*, aff. C-398/15, ECLI:EU:C:2017:197.

6 CE, 6 déc. 2019, M. A. c/ CNIL, n°391000, n°393769 n°395335, n°397755, n°399999, n°401258, n°403868, n°405464, n°405910, n°407776, n°409212 n°429154, n°423326.

7 CJUE, 24 sept. 2019, *Google c/ CNIL*, aff. C-507/17, ECLI:EU:C:2019:772.

8 Civ. 1re, 27 nov. 2019, FS-P+B+R+I, n° 18-14.675.

9 CE, 18 mars 2019, n°406313.

traitement des données à caractère personnel la concernant ». Partant, la position adoptée par le Conseil d'Etat apparaît particulièrement proche de la notion d'intérêt légitime, telle qu'elle est mentionnée dans le RGPD. On dénombre près d'une vingtaine d'affaires qui ont été jugées par le Conseil d'Etat sur la notion d'intérêt légitime dans le cadre d'une procédure portant sur le droit d'opposition. Il n'en demeure pas moins que la notion d'« intérêts légitimes » mentionnée à l'article 6.1 du RGPD n'a pas encore fait l'objet d'une interprétation des juridictions nationales.

En ce qui concerne le **consentement,** c'est surtout la CNIL qui s'est prononcée sur cette notion. En vertu de l'article 2, point h) de la directive 95/46/CE, le consentement s'entend comme toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. À cet égard, la notion de consentement, reprise dans le RGPD est d'ailleurs plus exigeante dès lors qu'il est prévu que celui-ci doit être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant.[10]

Il est à noter que le Tribunal de grande instance de Paris s'est prononcé sur 38 clauses des «Conditions d'utilisation » et des « Règles de confidentialité » de Google qu'il a déclaré comme abusives et certaines de ces clauses portaient sur le consentement des utilisateurs. En effet, la rédaction de ces clauses faisait apparaître qu'il y avait une présomption de consentement du consommateur à la collecte de ses données personnelles.

Le consentement a aussi été au cœur de la première condamnation de la CNIL post RGPD qui a été rendue contre Google le 21 janvier 2019.[11]

Question 5

Cette question a fait l'objet de débats, spécialement dans le cadre de l'adoption de la directive relative à certains aspects des contrats de fourniture du contenu numérique en avril 2019 (Directive 2019/770/UE).[12] La proposition initiale de la directive ne considérait le prix à payer pour la fourniture d'un contenu numérique que comme une somme d'argent. Or, l'économie numérique est fondée sur la donnée et la fourniture de données à caractère personnel constitue parfois le seul prix à payer. La fourniture de données à caractère personnel a été réintroduite par le compromis adopté au Conseil et la directive s'appliquera désormais lorsque le consommateur fournit uniquement des données à caractère personnel. Les services de communication interpersonnelle par contournement, les contrats groupés

10 Délibération CNIL n°2013-4203 du janvier 2014; Délibération CNIL n°MED-2018-023 du 25 juin 2018; Décision CNIL n°MED-2018-02325 du juin 2018.

11 Délibération n°SAN-2019-001 du 21 janvier 2019.

12 JOUE du 22 mai 2019, *L 136,* 22.5.2019, p. 1–27.

et le traitement des données à caractère personnel sont inclus dans le champ d'application de la directive relative au contenu numérique. À l'issue des négociations, une référence expresse au règlement général sur la protection des données personnelles (RGPD) a été introduite dans la directive (voir notamment le considérant 37 et l'article 3§8).

Ces enjeux ont aussi fait l'objet de discussions au Sénat en France lors de la présentation du rapport d'information n° 326 (2017-2018) de M. André Gattolin et Mme Colette Mélot, fait au nom de la commission des affaires européennes, déposé le 21 février 2018.[13]

Notons que la Quadrature du net, association de défense des libertés fondamentales dans l'environnement numérique, a défendu la position de ne pas considérer les données personnelles comme une marchandise et de ne pas les introduire dans la directive sur la fourniture de contenus numériques.[14] Le considérant 24 de la directive précise au contraire que: "tout en reconnaissant pleinement que la protection des données à caractère personnel est un droit fondamental et que, par conséquent, les données à caractère personnel ne peuvent être considérées comme des marchandises, la présente directive devrait garantir aux consommateurs, dans le cadre de ces modèles commerciaux, le droit à des recours contractuels". L'article 3§1 porte sur le champ d'application et pose ainsi que la directive s'applique lorsque le professionnel fournit ou s'engage à fournir un contenu numérique ou un service numérique au consommateur et le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, sauf lorsque les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel pour fournir le contenu numérique ou le service numérique ou pour permettre au professionnel de remplir les obligations légales qui lui incombent.

Question 6

L'article 10 de la nouvelle LIL pose que "aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception: 1° des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22."

13 Voir: http://www.senat.fr/rap/r17-326/r17-326_mono.html#toc8.

14 Cette association appelle à la reconnaissance d'un principe fondamental que le droit à la vie privée et à la protection des données, tout comme n'importe quel autre droit fondamental, ne puisse être vendu: https://www.laquadrature.net/2017/11/21/contenu_num_pe.

Exceptions prévues par le RGPD

Si cette partie de la LIL reprend le RGPD, il faut toutefois noter une formulation différente entre le RGPD et la version française. Alors que le RGPD accorde clairement un droit au profit de la personne concernée, "de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire", la LIL affirme qu'aucune décision ne peut être prise, ce qui semble être une obligation s'adressant au responsable de traitement, sans pour autant qu'il en soit explicitement débiteur. La reconnaissance d'un droit subjectif qui peut être mis en œuvre par un créancier de l'obligation a sans doute plus de vigueur qu'une formulation générale impersonnelle de nature à créer une obligation non explicitée à l'égard du responsable de traitement. Cette remarque doit toutefois être nuancée par le fait que cette disposition de la LIL s'intègre au chapitre V de la loi n° 2018-493 du 20 juin 2018 relatif aux "Dispositions particulières relatives aux droits des personnes concernées". L'intention du législateur français n'est certainement pas de remettre en cause ce droit consacré par le RGPD mais on pourra regretter qu'il n'ait pas repris la même formulation. La forme de la LIL s'explique cependant par la conservation de l'expression précédente prévue par la loi de 1978. Au demeurant, le CEPD a bien précisé que l'article 22 consacre une interdiction.[15]

Garanties supplémentaires

Parmi les différences, il faut également relever que la LIL ajoute une condition tenant au fait que "les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre" doivent être "communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande". Cette disposition renforce la protection de la personne concernée, ce qui est compatible avec un des objectifs du RGPD. On peut donc dire que le législateur français a adopté des mesures supplémentaires de sauvegarde des droits, libertés et légitimes intérêts des personnes concernées, y compris dans le cadre des exceptions prévues par le RGPD.

Une telle disposition traduit la volonté de reconnaître explicitement un droit à la transparence et à l'explication qui est sous-entendu dans le RGPD et a fait l'objet de débats, surtout parmi la doctrine aux États-Unis et en Europe sur le fait de savoir s'il existe ou

15 CEPD, Lignes directrices sur la prise de décision individuelle automatisée et le profilage, WP 251, 6 févr. 2018, p. 21.

non un droit à explication à l'article 22 du RGPD,[16] complété par les articles 13-15.[17] Il semble qu'il faille distinguer le droit à l'information, clairement consacré dans le RGPD, et le droit individuel à explication qui n'est pas visé dans le RGPD lui-même mais uniquement au considérant 71. Ce débat a peu été repris en France pour des raisons expliquées ci-après.

Dispositions spécifiques à la France non directement liées au RGPD

La loi précitée n° 2016-1321 *Pour une République numérique* (ci-après LRN) posait déjà des règles relatives à la transparence des décisions automatisées prises par l'administration.[18] Elle contenait deux catégories de règles à l'égard des plateformes numériques, d'une part, et des administrations, d'autre part. La loi du 20 juin 2018 est venue modifier les secondes. La LRN a créé un nouvel article L. 311-3-1 du Code des relations entre le public et l'administration (CRPA), selon lequel:

> "*une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande*". Ce droit à l'information a été précisé par décret.[19]

16 B. Goodman and S. Flaxman, EU Regulations on Algorithmic Decision-Making and A « right to Explanation » (2016): https://arxiv.org/abs/1606.08813; B. Goodman, A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection, 29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelone, Espagne; M. Hildebrandt, The New Imbroglio – Living with Machine Algorithms, *in* The Art of Ethics in the Information Society (2016). S. Wachter, B. Mittelstadt, L. Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation?, International Data Privacy Law, 7(2), 76–99 (2017). Andrew D. Selbst and Julia Powles, Meaningful Information and the Right to Explanation, International Data Privacy Law, vol. 7(4), 233-242 (2017). Voir aussi: L. Edwards et M. Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, Duke Law & Technology Review, à paraître.

17 Rappelons que l'article 15h) du règlement consacre le droit d'obtenir du responsable de traitement des informations sur l'existence d'une prise de décision automatisée, y compris un profilage, mais aussi « au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

18 J.-M. Pastor, Accès aux traitements algorithmiques utilisés par l'administration, *AJDA* 2017, 604.

19 Un décret n° 2017-330 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique a été pris le 14 mars 2017 pour préciser l'obligation de communication. Il indique désormais à l'article R. 311-3-1-2 du code des relations entre le public et l'administration (CRPA) que: « l'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes: le degré et le mode de contribution du traitement algorithmique à la prise de décision; les données traitées et leurs sources; les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé; les opérations effectuées par le traitement ». Ce droit d'accès peut s'exercer auprès de toute administration, y compris des collectivités territoriales, « *sous réserve de ne pas porter atteinte à des secrets protégés par la*

En outre, l'article 6 de la LRN prévoit que

> "*Sous réserve des secrets protégés, les administrations (…) publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles*".

La possibilité ainsi laissée de se prévaloir des secrets risque de vider de sa substance le principe de la diffusion de l'information. Dans son avis sur le projet de loi,[20] le Conseil d'Etat avait d'ailleurs mis en garde contre une trop grande précision des informations données dans ce cadre à même de "*permettre à des usagers de se constituer un profil permettant de contourner les prescriptions qui seraient applicables aux opérateurs* ". Rappelons, en outre, que le considérant 63 encadre cette exception qui ne doit pas faire obstacle à la transparence.[21]

Intégration de ces dispositions spécifiques dans le cadre de l'exception permise par le RGPD (art. 22§2b)

Le législateur français a profité de la flexibilité offerte par l'article 22§2 b) du RGPD pour modifier ces dispositions et renforcer l'exception en droit national au droit de ne pas faire l'objet d'une décision automatisée comme le montre nouvel article 10 de la LIL.

Garanties pour les personnes concernées

S'agissant des mesures de sauvegarde des droits, libertés et légitimes intérêts des personnes concernées, la nouvelle LIL prévoit un droit individuel à explication qui témoigne d'une sur-adaptation du RGPD par le législateur français.

Interprétation et garanties précisées par le Conseil constitutionnel

Le Conseil constitutionnel a précisé que

> "*ces dispositions se bornent à autoriser l'administration à procéder à l'appréciation individuelle de la situation de l'administré, par le seul truchement d'un algorithme, en fonction des règles et critères définis à l'avance par le*

---

loi » mais aussi dans les limites des restrictions et secrets énumérés au 2° de l'article L. 311-5 du CRPA. Enfin, le silence gardé par l'administration au terme du délai d'un mois vaut décision de rejet (CRPA, art. R. 311-12 et R. 311-13) du CRPA.

20 Avis du 3 déc. 2015, n° 390741.

21 Le considérant 63 du RGPD indique que le droit d'accès accordé à l'article 15 du RGPD « *ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée* ».

> *responsable du traitement. Elles n'ont ni pour objet ni pour effet d'autoriser l'administration à adopter des décisions sans base légale, ni à appliquer d'autres règles que celles du droit en vigueur. Il n'en résulte dès lors aucun abandon de compétence du pouvoir réglementaire*".[22]

En outre, le seul recours à un algorithme pour fonder une décision administrative individuelle est subordonné au respect de trois conditions:

1. d'une part, conformément à l'article L. 311-3-1 du CRPA, la décision administrative individuelle doit mentionner explicitement qu'elle a été adoptée sur le fondement d'un algorithme et les principales caractéristiques de mise en œuvre de ce dernier doivent être communiquées à la personne intéressée, à sa demande. Il en résulte que, lorsque les principes de fonctionnement d'un algorithme ne peuvent être communiqués sans porter atteinte à l'un des secrets ou intérêts énoncés au 2° de l'article L. 311-5 du code des relations entre le public et l'administration, aucune décision individuelle ne peut être prise sur le fondement exclusif de cet algorithme.
2. D'autre part, la décision administrative individuelle doit pouvoir faire l'objet de recours administratifs, conformément au chapitre premier du titre premier du livre quatrième du CRPA. L'administration sollicitée à l'occasion de ces recours est alors tenue de se prononcer sans pouvoir se fonder exclusivement sur l'algorithme. La décision administrative est, en outre, en cas de recours contentieux, placée sous le contrôle du juge, qui est susceptible d'exiger de l'administration la communication des caractéristiques de l'algorithme.
3. Enfin, le recours exclusif à un algorithme est exclu si ce traitement porte sur l'une des données sensibles mentionnées au paragraphe I de l'article 8 de la LIL qui reprend l'article 9 du RGPD).

Par ailleurs, le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement. Au vu de tous ces éléments, le Conseil constitutionnel a estimé que le législateur a défini des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme.

Le Conseil constitutionnel a ainsi réduit les risques liés à l'utilisation d'un algorithme protégé par un secret ou un droit de propriété intellectuelle, lesquels secret et droit ne

22 CC décision n° 2018-765 DC du 12 juin 2018 (pts 69-72).

pourraient faire obstacle à la transparence. Il a également précisé les conditions d'un recours contre une décision prise sur le fondement d'un algorithme et le fait que l'explication doit être apportée par un humain et non par un algorithme et sous contrôle judiciaire. Cela suppose donc que le type d'algorithme utilisé soit maîtrisable et explicable, ce qui exclut les outils auto-apprenants dits *machine learning* qui "apprennent" et évoluent sans contrôle humain. Enfin, l'exclusion des données sensibles doit permettre d'éviter le risque d'une discrimination algorithmique fondée sur des données biaisées concernant par exemple les origines ethniques. Si ces dispositions vont dans le bon sens pour limiter les risques de discrimination amplement relevés par la doctrine, notamment aux États-Unis,[23] de tels risques ne peuvent être totalement éliminés puisque d'autres facteurs en apparence objectifs peuvent conduire à des résultats biaisés et discriminants. Ces facteurs dits "proxies" peuvent être indirectement porteurs d'informations sensibles, comme par exemple le code postal qui révèle souvent un niveau social voire une origine ethnique.

Décisions de justice

Par ailleurs, il faut remarquer que le début de l'article 10 de la LIL précise que "aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne". Cette disposition n'est pas nouvelle et était déjà consacrée par la loi n° 78-27 du 6 janvier 1978.[24] Une évaluation automatisée des caractéristiques d'une personne conduisant à une décision ne peut être réalisée sur la seule base de cette évaluation. Cela suppose donc que d'autres critères soient pris en compte ou encore que d'autres moyens soient utilisés *a minima* en complément pour aider la prise de décision et non pour la prendre.

Question 7

L'exercice du droit à l'effacement, tel qu'il ressort de l'article 17 du RGPD et 12 de la directive 95/46/CE, a connu une application renforcée depuis l'arrêt *Google Spain* de 2014 rendu par la Cour de justice de l'Union européenne.

En ce qui concerne le droit au déréférencement, il est possible de constater que le contentieux qui s'y rapporte met en évidence, à la fois, un renforcement de la protection

23 Voir par exemple S. Barocas et A. Selbst, 'Big Data's Disparate Impact', *Cal. L. Rev*. Vol. 104, No. 3 (2016), pp. 671-732; A. Chander, 'The Racist Algorithm?', *Mich. L. Rev*. Vol. 115, No. 6 (2017), pp. 1023-1045.

24 L'art. 10 de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 prévoyait ainsi que: « *Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

des droits des personnes physiques et le détermination d'un équilibre entre les droits des personnes physiques et le droit à l'information.

Dans une délibération de 2016,[25] la CNIL a infligé une sanction à Google de 100,000 euros pour avoir refusé de mettre en œuvre des demandes bien fondées de déréférencement de personnes physique sur l'ensemble des extensions de noms de domaine de son moteur de recherche. Les juridictions administratives ont adopté une position similaire sur le « droit au déréférencement » en imposant à des sociétés de répondre favorablement à des demandes de particuliers.[26]

La Cour de justice a rendu une décision le 24 septembre 2019 consacrant le champ européen et non mondial du « droit au déréférencement ».[27] Dans un autre arrêt rendu le même jour, la Cour de justice a également donné des éléments sur les conditions dans lesquelles les personnes peuvent obtenir le déréférencement d'un lien apparaissant dans un résultat de recherche lorsque la page auquel le lien renvoie contient des informations relatives à des informations sensibles.[28]

Les juridictions judiciaires connaissent des problématiques similaires. Elles tentent de trouver un juste équilibre entre la protection des droits des personnes et le droit à l'information. Ainsi, dans une ordonnance de référé du 19 décembre 2014 le TGI de Paris considère que la demanderesse « justifie de raisons prépondérantes et légitimes prévalant sur le droit à l'information ».[29] D'ailleurs, la Cour de cassation a également censuré dans une décision du 27 novembre 2019 un arrêt d'une Cour d'appel qui avait rejeté une demande de déréférencement faite par un particulier auprès de Google.[30]

Question 8

Dès son origine en 1978 la LIL comportait une dérogation pour les traitements relatifs à la liberté d'expression qui a été modifié pour l'adapter à l'article 85 RGPD. L'article 80 de la LIL actuelle pose néanmoins trois séries de questionnements relatifs à sa conformité au RGPD:

– l'article 80 LIL reste assez vague en ce sens qu'il ne saurait à lui seul permettre véritablement de concilier le droit à la protection des données avec la liberté d'expression. Le parti pris de l'adaptation française a donc été de considérer que l'article 85§1 ne posait pas d'obligation spécifique d'adopter une loi sur ce sujet. L'article 80 se

25 Délibération n°2016-054 du 10 mars 2016 de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X.

26 Conseil d'État, 10ème - 9ème chambres réunies, 19 juillet 2017, n° 399922.

27 CJUE, 24 sept. 2019, *Google c/ CNIL, préc.*

28 CJUE, 24 sept. 2019, *GC e.a. c/ CNIL*, aff. C-136/17, ECLI:EU:C:2019:773.

29 TGI Paris, Ord., 24 novembre 2014, Marie-France M. / Google France et Google Inc.

30 Civ. 1re, 27 nov. 2019, *préc.*

contente de dresser la liste des droits qui peuvent faire l'objet d'une dérogation pour les quatre finalités prévues par l'article 85§2 RGPD.
- l'adaptation continue comme précédemment à se concentrer essentiellement sur les traitements à des fins journalistiques et n'apporte aucune explication, définition relative aux autres finalités de traitement visés par l'article 85 RGPD (traitement à des fins d'expression universitaire, artistique ou littéraire).
- l'article 80 LIL n'est pas conforme à la lettre du RGPD dans la mesure où il maintient comme auparavant que les restrictions ne concerne que les traitements mis en œuvre "aux fins d'exercice *à titre professionnel* [mis en italique par nous], dans le respect des règles déontologiques de cette profession" alors que cette la référence au caractère professionnel n'existe pas à l'article 85 §2 du RGPD. Autrement dit, le droit français ne permet pas l'application de ces dérogations aux journalistes blogueurs ne disposant pas de carte professionnelle, voire les robots-journalistes. Pourtant, la CJUE a une approche large de la notion d'activité de journalisme incluant « *la divulgation au public, sous quelque moyen de transmission que ce soit, d'informations, d'opinions ou d'idées* ».[31] L'approche française est bien plus centrée sur le journalisme et les médias classiques.

Les dérogations permises pour les traitements relevant des quatre finalités de l'article 85 RGPD sont:
- des dérogations à l'interdiction de traitement de données sensibles (article 9 RGPD) ou des traitements de condamnation (article 10 RGPD)
- des dérogations au droit à l'information, au droit d'accès, mais aussi au droit de rectification et de limitation. En revanche, aucune limitation au droit d'opposition, ni au droit de portabilité, ni à l'article 22 RGPD n'ont été prévues.

L'article 80 de la LIL rappelle, par ailleurs, que la mise en œuvre d'une telle dérogation ne remet pas en cause les règles de droit interne relatives à la possibilité d'exercer un droit de réponse ou de se voir dédommager en cas d'atteinte à la vie privée ou à la réputation des personnes.

Au-delà de l'article 80 de la LIL:
- l'article 19 de LIL rappelle que la CNIL doit exercer ses pouvoirs notamment de contrôles en respectant « *le secret des sources des traitements journalistiques* ».
- En dehors de la LIL, la France a adopté plusieurs lois récemment visant à encadrer la liberté d'expression sur internet, telles que deux lois sur les *fake news*.[32] La proposition

31 CJUE 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, aff. C-73/07, EU:C:2008:727, point 61 CJUE, ou encore CJUE, 14 février 2019, *Sergejs Buivids*, aff. C-345/17, ECLI:EU:C:2019:122, point 59.

32 Loi organique n°2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, Loi n° 2018-120 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

de loi contre les discours de haine sur Internet actuellement en cours de discussions est au cœur d'un vif débat politique sur l'interdiction ou le maintien de l'anonymat sur Internet.[33]

C Application interne de la législation en matière de protection des données

Question 9

En France, l'autorité de contrôle est la Commission Nationale Informatique et Libertés (ci-après « CNIL »). Il s'agit d'une autorité administrative indépendante au sens de la loi n° 2017-55 qui ne dispose pas de la personnalité juridique. La CNIL est composée d'un collège pluridisciplinaire de 18 membres dont 9 membres sont désignés par des organes politiques (Parlement, gouvernement). Le Président de la CNIL est nommé par le Président de la République, après validation de son candidat par les deux chambres du parlement. Mme Marie- Laure Denis est la présidente actuelle de la CNIL depuis janvier 2019. Le mandat des commissaires est de 5 ans ou, pour les parlementaires, d'une durée égale à leur mandat électif. Il n'existe aucune restriction d'âge, ni de renouvellement.

La CNIL est actuellement composée de:

- **4 parlementaires** (2 députés, 2 sénateurs)
- **2 membres du Conseil économique, social et environnemental**, élus par cette assemblée
- **6 représentants des hautes juridictions** (2 conseillers d'État, 2 conseillers à la Cour de cassation, 2 conseillers à la Cour des comptes) élus par leur assemblée générale respectives
- **5 personnalités qualifiées** désignées par le Président de l'Assemblée nationale (1 personnalité), le Président du Sénat (1 personnalité), en Conseil des ministres (3 personnalités). Ces personnes sont choisies pour leur connaissance du numérique et des questions touchant aux libertés individuelles.
- **Le Président de la CADA** (Commission d'accès aux documents administratifs),

En outre, le défenseur des droits y participe avec une voix consultative.

La CNIL est structurée de manière à assurer une séparation fonctionnelle entre sa mission de régulation et de contrôle. Elle comporte:

33 cf. Voir dossier législatif: www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.

- **une formation plénière** dont la compétence principale est d'établir la doctrine de la CNIL (avis, lignes directrices, autorisation, certification, agrément, référentiel, code de conduite, clauses contractuelles, règlement intérieur etc.). Les décisions sont prises à la majorité absolue des membres présents. Un Commissaire du gouvernement assiste à la réunion plénière.
- **un bureau:** composé de la présidente et de deux Vice-Présidents. Le bureau peut, à la demande du président de la CNIL **rendre publique une mise en demeure** prise à l'encontre d'un responsable de traitement ne respectant pas les obligations issues de la LIL, il habilite les agents de la CNIL pouvant exercer des contrôles, etc.
- une **formation restreinte** à laquelle aucun membre du bureau ne participe. Cette formation restreinte est composée de 6 membres élus au sein du collège de la CNIL. La formation restreinte dispose de son propre président. Elle assure la fonction de contrôle de la CNIL (prise de mesures et sanctions).

En ce qui concerne ses missions, la CNIL assume des missions d'information, de recommandation et de contrôle. Quelques spécificités:

- La CNIL peut certifier "*des personnes et des produits, des systèmes de données ou de procédures aux fins de reconnaître qu'ils sont conformes au RGPD*", soit directement, soit par l'intermédiaire d'un organisme accrédité. Le champ de la certification va delà de ce qui a été accepté par le CEPD dans ses lignes directrices. Ce dernier refuse d'appliquer la certification aux personnes et notamment aux DPO. Pourtant, la CNIL vient de procéder à l'agrément de l'AFNOR pour certifier les DPO sur la base de référentiels.[34]
- Doit sensibiliser les médiateurs de la consommation et les médiateurs publics
- Promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement

Le budget de la CNIL en 2019 est de 18,5 millions €, nombre d'employés 215. La majorité des membres et du personnel de la CNIL ont un profil de juriste. Malgré une hausse de son budget, la CNIL considère qu'elle n'a pas suffisamment de moyens pour répondre à l'ensemble de ses missions.

34 CNIL, délibération n° 2018-317 du 20 septembre 2018 *portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO)* et CNIL, délibération n° 2018-318 du 20 septembre 2018 *portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données* (DPO) et CNIL, délibération n° 2018-317 du 20 septembre 2018 *portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO*), *JORF* n°235 du 11 octobre 2018 et Délibération n°2019-092 du 4 juillet 2019 portant agrément d'AFNOR CERTIFICATION pour la certification des compétences du délégué à la protection des données (DPO).

Question 10

La nouvelle LIL ne prévoit pas de dispositions particulières relatives au traitement des plaintes. En revanche, le chapitre VI du règlement intérieur de la CNIL prévoit des dispositions en la matière (articles 47 à 51).

Est considérée comme une plainte toute demande formée par une personne physique ou morale identifiée relative à des faits susceptibles d'être contraires aux textes dont l'application est confiée à la Commission. Les plaintes sont instruites par les services de la Commission (article 47).

La Commission peut être saisie par voie postale ou électronique. Le plaignant indique son nom et ses coordonnées sur la plainte (article 48).

Si la demande concerne l'exercice des droits d'accès, de rectification ou d'opposition prévus par la loi du 6 janvier 1978 modifiée, et que le plaignant n'a pas cherché à exercer ses droits directement auprès du responsable du traitement, les services de la Commission lui adressent un courrier l'informant des démarches qu'il lui appartient d'engager préalablement à toute saisine de la Commission (article 49).

L'objet de la plainte est communiqué au responsable du traitement mis en cause, ou, le cas échéant, au correspondant, afin que celui-ci fournisse toutes les explications utiles. Ces échanges peuvent avoir lieu par tout moyen.

Selon le rapport annuel de la CNIL, 11077 plaintes ont été déposées devant la CNIL en 2018, soit une augmentation de 32% liée à l'entrée en application du RGPD et à la sensibilisation qui l'a accompagnée. Ces plaintes ont fait l'objet de 6609 vérifications indirectes et 4264 demandes de droit d'accès indirect.

Question 11

Application des sanctions par la CNIL[35]

La CNIL dispose d'une chaîne répressive complète lui permettant de recevoir des signalements par des canaux divers, de réaliser des contrôles dont les suites peuvent aller de la clôture, à la mise en demeure ou à la sanction financière ou non. Dans certains cas, une **publicité** peut être décidée en fonction de la gravité des cas.

Le signalement peut provenir d'une plainte, autosaisine, faits signalés par la presse ou par le signalement des autres autorités nationales de contrôle des autres États membres.

La CNIL a le pouvoir d'effectuer des contrôles auprès de l'ensemble des organismes qui traitent des données à caractère personnel, soit les entreprises privées, associations ou

35 Source: site de la CNIL., https://www.cnil.fr/fr/mission-4-controler-et-sanctionner.

encore organismes publics. Ces contrôles peuvent se dérouler sur place, sur pièces, sur audition ou en ligne.

À l'issue de contrôle ou plaintes, en cas de méconnaissance des dispositions du RGPD ou de la loi n° 78-17 de la part des responsables de traitement et sous-traitants, la formation restreinte de la CNIL peut prononcer des **sanctions** à l'égard des responsables de traitements qui ne respecteraient pas ces textes.

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut:

- Prononcer un rappel à l'ordre;
- Enjoindre de mettre le traitement en conformité, y compris sous astreinte;
- Limiter temporairement ou définitivement un traitement;
- Suspendre les flux de données;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte;
- Prononcer une amende administrative (voir le RGPD).

Ces sanctions peuvent être rendues publiques.[36]

À compter de la date de notification de la décision de la formation restreinte, l'organisme mis en cause dispose d'un délai de deux mois pour former un recours devant le Conseil d'État contre la décision de la CNIL.

Notons que le Président de la CNIL peut adresser à un responsable de traitement ou à un sous-traitant une **mise en demeure** de cesser un ou plusieurs manquement(s) constaté(s) au RGPD dans un délai fixé. Elle intervient après une plainte reçue par la CNIL ou un contrôle (en ligne ou sur place) effectué auprès d'un organisme. Une mise en demeure n'est pas une sanction. Une mise en demeure peut-être publique.[37] Dans ce cas, le bureau de la CNIL, composé du Président et des vice-présidents, adopte une délibération dans laquelle il explique les raisons pour lesquelles il décide de rendre publique la mise en demeure. La mise en demeure publique fait l'objet d'un communiqué synthétique sur le site de la CNIL et la décision est publiée sur Légifrance. Celle-ci est anonymisée au bout de 2 ans, mais reste toujours accessible sur Légifrance. Si l'organisme s'est mis en conformité, la clôture de la mise en demeure est également rendue publique et anonymisée au bout de deux ans.

D'après le rapport annuel de la CNIL, 310 contrôles ont été effectués en 2018 avec 11 sanctions prononcées, dont 9 sanctions pécuniaires publiques, 1 avertissement non public et un non-lieu.

36 Pour des exemples, voir: www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil.

37 Pour des exemples, voir: www.cnil.fr/fr/thematique/cnil/mises-en-demeure.

Par ailleurs, 11077 plaintes ont été déposées, soit une augmentation de 32% et un chiffre record lié à l'entrée en application du RGPD.

Sanctions additionnelles

Les sanctions additionnelles sont prévues à l'article 84§1 du RGPD. Le paragraphe 2 précise que chaque État membre doit notifier à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

Les sanctions pénales en cas de manquement aux règles en matière de protection des données étaient déjà prévues en droit français avant l'adoption du RGPD et réprimées par les articles 226-16 à 226-24 du Code pénal (section 5 du chapitre VI du titre II du livre II du code pénal). Elles peuvent aller jusqu'à une amende de 300 000 euros et 5 ans d'emprisonnement.

L'article 41 de la loi n° 78-17 de la nouvelle LIL dispose que "le procureur de la République avise le président de la Commission nationale de l'informatique et des libertés de toutes les poursuites relatives aux infractions prévues par la section 5 du chapitre VI du titre II du livre II du code pénal et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours

Question 12

Le droit français prévoit effectivement une indemnisation des préjudices moraux avec l'octroi de dommages-intérêts. Généralement, les actions sont fondées sur les articles 1240 et 1241 nouveaux du code civil et non sur la LIL. Il découle des principes régissant responsabilité civile délictuelle que le préjudice doit être réparé dans son intégralité, sans toutefois excéder le montant de ce préjudice. Or, aucune disposition ne prévoit une sanction spécifique ou un montant en cas de préjudice moral. Une analyse de la jurisprudence montre qu'en raison du fait que le préjudice moral est difficilement quantifiable, la réparation de celui se fait selon une « logique rétributive et non réparatrice par volonté de dissuasion d'actes jugés antisociaux ».[38] Au demeurant, la réparation du préjudice moral repose sur une appréciation *in concreto* de la situation. Dès lors, pour obtenir réparation d'un tel préjudice, il convient de vérifier l'existence de conditions de mise en jeu de la responsabilité civile délictuelle, c'est-à-dire l'existence d'une faute, d'un dommage et d'un lien de causalité entre les deux.

38 F. Gras, « L'indemnisation des atteintes à la vie privée », *LEGICOM*, Vol. 20, No. 4, 1999, pp. 21-25.

Une analyse de la jurisprudence montre que les juridictions ne suivent pas de règles spécifiques pour établir le montant du préjudice moral qu'elles accordent à la victime. Certaines juridictions accordent des indemnisations sans justifier le choix du montant.[39] Parfois, les juridictions procèdent à une analyse *in concreto* pour évaluer le montant de la somme pour l'indemnisation d'un préjudice moral par exemple.[40]

Question 13

En France, l'action de groupe en matière de protection des données à caractère personnel a été introduite en 2016 par la LRN. Elle ne concernait que l'action en cessation de manquement. Le nouvel article 37 III de la LIL y ajoute désormais une action en réparation. La France a ainsi utilisé la clause ouverte laissée par l'article 80 §1 du RGPD. Les organismes concernés sont les associations déclarées, les associations agréées, les organisations syndicales de salariés ou de fonctionnaires, (cf. article 37 IV LIL) qui peuvent agir avec (article 38 LIL) ou sans mandat de la personne concernée. (article 80 §2 RGPD)

L'article 37 de la LIL pose néanmoins plusieurs difficultés de conformité[41] au regard du RGPD:

- D'une part, il limite explicitement les personnes à qui un mandat peut être donné: Associations régulièrement déclarées depuis 5 ans. Cette limitation issue du droit antérieur français n'a pas été supprimée, alors qu'il n'existe aucune limite temporelle dans le RGPD, (sous-adaptation du droit français).
- D'autre part, le droit français permet une action de groupe en réparation y compris lorsque la personne concernée n'a pas donnée de mandat. Or, l'article 80 §2 RGPD n'évoque une telle possibilité que pour une action en cessation de violation. (Sur-adaptation du droit français).

39 CA Paris, Pôle 5 – Ch. 1, 7 mars 2017, *Sound Strategy / Concepson*. En ce sens également: TGI Clermont-Ferrand, Chambre correctionnelle Jugement du 26 septembre 2011, *Sociétés X. et Y. / Mme Rose*; TGI de Paris, 17e ch., 21 novembre 2018, *Mme X. / Sarl Denim*.

40 CA Paris, pôle 5 – chambre 1, 10 mars 2015, Stéphane B. / Artnet France et Artnet Worldwide Corporation.

41 cf. Alexia Pato, The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Rights, blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf.

Dans la pratique, l'association Que Choisir?[42] et l'association la Quadrature du net[43] ainsi que l'Open Internet Society France[44] sont les trois entités françaises à s'être emparées de ces possibilités d'actions collectives.

Notons, qu'au-delà de la multiplication des associations de DPO,[45] un syndicat des DPO a vu le jour en France en avril 2019.[46] Sa vocation est de protéger la profession des DPO, notamment dans leurs possibles conflits avec leurs employeurs responsables de traitements ou sous-traitants et de favoriser les médiations.

Question 14

Le développement du numérique a forcé les autorités nationales à mettre en place une meilleure coordination et coopération entre les différents régulateurs. Le 24 juin 2019, plusieurs régulateurs (l'Autorité de la concurrence, l'Autorité des marchés financiers, l'Autorité de régulation des activités ferroviaires et routières, l'Autorité de régulation des communications électroniques et des postes, la Commission nationale de l'informatique et des libertés, la Commission de régulation de l'énergie et le Conseil supérieur de l'Audiovisuel) se sont réunis afin de mettre en place des mutualisations entre ces autorités.[47] Ces mutualisations portent sur différents thèmes tels que la commande publique, la gestion des connaissances et les ressources humaines. Cette rencontre a permis d'établir un rapport rendu public le 8 juillet 2019 sur leur approche commune de « la régulation par la donnée ».[48]

L'objectif de cette coopération est de développer une régulation par la donnée afin de permettre aux différents régulateurs d'acquérir de nouvelles compétences en matière d'échange de données ou encore d'appropriation de nouvelles technologies. Il ressort du rapport que le développement des nouvelles technologies engendre pour les régulateurs "de nouveaux besoins en compétence technique, notamment en matière d'analyse de données et d'algorithmes mais également de stockage et gestion de gros volumes de données.

42 www.quechoisir.org/action-ufc-que-choisir-vie-privee-donnees-personnelles-action-de-groupe-contre-google-n68403/: Première action de groupe devant le TGI de Paris en juin 2019.

43 gafam.laquadrature.net/: première plainte collective (art. 77 RGPD) en mai 2018.

44 www.lefigaro.fr/secteur/high-tech/la-premiere-action-de-groupe-contre-facebook-en-france-sera-lancee-en-septembre-20190327.

45 A côté de l'ancienne Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCPD), l'Association des Data Protection Officers créée en 2016, et l'Union des Data Protections Officers.

46 Syndicat Français des Experts en protection des données et Data Protection Officers.

47 www.cnil.fr/fr/cooperations-entre-regulateurs.

48 www.cnil.fr/sites/default/files/atoms/files/note-aai-regulation-par-la-data-juil2019.pdf.

D Traitement de données pour des motifs de sécurité nationale

Question 15

En droit français la notion de « sécurité nationale » est définie, à l'art. L 1111-1 du code de la défense.

Les autorités françaises ont manifesté une grande réticence à l'application des décisions *Tele2 et Watson*. Elles considèrent que la conservation des données est nécessaire afin de pouvoir faire face aux menaces. Cette conviction relative à l'utilité de la conservation des données se reflète dans les questions préjudicielles posées par le Conseil d'Etat dans les affaires en cours initiés à l'échelle nationale par la Quadrature du Net (aff. C-511 et C-512/18). Ces interrogations sont assez proches de celles qui sont à l'origine d'autres questions préjudicielles C-623/17 (International Privacy), C-520/18 (Ordre des barreaux francophone et germanophone) qui sont pendantes devant la CJUE.[49]

49 Affaire C-520/18: Demande de décision préjudicielle présentée par la Cour constitutionnelle (Belgique) le 2 août 2018 — Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX/ Conseil des ministres JO C 408 du 12.11.2018, p. 39–40; Affaire C-623/17: Demande de décision préjudicielle présentée par le Investigatory Powers Tribunal — London (Royaume-Uni) le 31 octobre 2017 — Privacy International/ Secretary of State for Foreign and Commonwealth Affairs e.a, JO C 22 du 22.1.2018, p. 29–30.

Germany

Dieter Kugelmann[*]

A Setting the Scene – Weichenstellung

Frage 1

Die Bundesrepublik Deutschland hat die Datenschutz-Grundverordnung (DS-GVO)[1] parallel zu ihrem Wirksamwerden am 25. Mai 2018 auf Bundesebene umgesetzt. In einem umfangreichen Artikelgesetz, dem 1. Datenschutz-Anpassungs- und Umsetzungsgesetz, wurde eine Reihe von Vorschriften der Bundesgesetze geändert. Im Zentrum stand die Neufassung des Bundesdatenschutzgesetzes (BDSG), die grundlegende Weichenstellungen enthält.[2] Auch wenn einige Bestimmungen des BDSG berechtigter Kritik begegnen,[3] sind damit Rahmenbedingungen und modellhafte Regelungen geschaffen worden, die für die weitere Gestaltung der Fachgesetze des Bundes und für die Gestaltung des Landesrechts Bedeutung entfalten.

Im Bundesstaat sind auch die Länder der Bundesrepublik verpflichtet, ihre Rechtsordnung entsprechend umzustellen. Die Länder haben das inzwischen alle getan, manche mit etwas Verspätung. Dies betrifft eine Reihe von Landesgesetzen und insbesondere die Landesdatenschutzgesetze. Vielfach haben sie sich am Bundes-Datenschutzgesetz orientiert.

Auf Bundesebene ist Ende 2019 das 2. Datenschutz-Anpassungs- und Umsetzungsgesetz in Kraft getreten, mit dem 154 Gesetze geändert werden.[4] Auch das Bundes-Datenschutzgesetz selbst erfährt einige Modifikationen. Am meisten Aufmerksamkeit hat die Änderung erfahren, dass die in § 38 Abs. 1 BDSG festgeschriebene Pflicht von Verantwortlichen einen Datenschutzbeauftragten zu benennen, nun nicht mehr ab 10 mit automatisierter Datenverarbeitung beschäftigten Personen entsteht, sondern

* Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Rheinland-Pfalz.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1.

2 Als Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz), BGBl. I 2017, S. 20197; dazu Greve, NVwZ 2017, 737; Kühling, NJW 2017, 1985.

3 Siehe die kritische Stellungnahme des Bundesrates, BR-Drs. 110/17.

4 BGBl. 2019 I, S. 1626.

erst ab 20 Personen. Diese Änderung verfolgt das Ziel, die behaupteten Belastungen kleinerer und mittlerer Unternehmen oder anderer Verantwortlicher wie Arztpraxen durch die DS-GVO zu verringern. Dabei wird in dieser weiter anhaltenden Diskussion oft vernachlässigt, dass die Pflicht zu Einhaltung der Vorschriften des Datenschutzrechts selbstverständlich besteht und ohne betrieblichen Datenschutzbeauftragten der Sachverstand zur Erfüllung dieser Pflicht beim Verantwortlichen gerade fehlen könnte.[5]

Die Öffnungsklauseln der Datenschutz-Grundverordnung eröffnen den Gesetzgebern Spielräume, um Besonderheiten des innerstaatlichen Rechts gerecht zu werden und besondere Interessenlagen zu berücksichtigen.[6] Diese Spielräume sind zwingend zu nutzen, um das innerstaatliche Recht in Einklang mit der Verordnung zu bringen.[7] Zentrales Instrument hierzu ist das Datenschutzgesetz. Die Datenschutzgesetze in Bund und Ländern sind an die Begriffe, Verständnisse und Regelungen der Datenschutz-Grundverordnung anzugleichen.

Von den Öffnungsklauseln der Datenschutz-Grundverordnung wurde in umfangreichem Maße Gebrauch gemacht. Dies betrifft insbesondere das Bundesdatenschutzgesetz, aber auch die Landesdatenschutzgesetze. Diese Erweiterungen sind unabhängig davon, dass nach Art. 6 Abs. 1 lit. c und e i.V.m. Abs. 3 DS-GVO die Gesetze zur Erfüllung öffentlicher Aufgaben auf ihre Vereinbarkeit mit der Datenschutz-Grundverordnung geprüft werden müssen. Zumeist sind die gesetzlichen Änderungen allerdings technischer Natur. Begriffe werden umgestellt („Verantwortlicher" statt „verantwortliche Stelle" usw.). Das europarechtliche Wiederholungsverbot, das der EuGH festgelegt hat, ist durchaus sehr weit verstanden worden. An mancher Stelle kann man anzweifeln, ob der nationale Gesetzgeber hier überzogen hat.[8]

Großen Bedenken begegnete von Beginn an der § 4 BDSG zur Videoüberwachung öffentlich zugänglicher Räume. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat bereits früh seine Vereinbarkeit mit dem vorrangigen Unionsrecht bestritten. Nunmehr hat das Bundesverwaltungsgericht festgestellt, dass der Anwendungsvorrang des Unionsrechts insoweit greift.[9] Im konkreten Fall stellt es fest, dass die Videoüberwachung in einer Arztpraxis an Art. 6 Abs. 1 lit. f DS-GVO zu messen ist. Der innerstaatliche Gesetzgeber hatte in § 4 BDSG eine stärkere Gewichtung von Sicherheitsinteressen in einer Reihe von

5 Ablehnend hierzu die Entschließung „Keine Abschaffung der Daten- schutzbeauftragten" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23.4.2019 (https://datenschutz-online.de). Hinweis: Die Fundstellen der Online-Quellen wurden zuletzt am 12.8.2019 besucht.

6 Albrecht/Jotzo, Das neue Datenschutzrecht der EU. Grundlagen – Gesetzgebungsverfahren – Synopse, 2017, S. 133.

7 Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel, Die Datenschutz-Grundverordnung und das nationale Recht, 2017, S. 1 f.

8 Kugelmann, DuD 2018, 482.

9 BVerwG, Urteil vom 27. März 2019 - BVerwG 6 C 2.18, DuD 2019, 518.

Situationen der Videoüberwachung, etwa von Einkaufzentren, Parkplätzen oder Sportstätten festgelegt. Diese Gewichtung enthält Art. 6 der DS-GVO nicht. Aus diesem Grunde ist § 4 BDSG unanwendbar. In der Konsequenz wird die Interessenabwägung nach Art. 6 Abs. 1 DS-GVO durchgeführt.

Die innerstaatlichen Datenschutzaufsichtsbehörden üben eine umfassende Aufsicht im Bereich der DS-GVO aus. Dies betrifft auch die Nutzung der Öffnungsklauseln. Daher haben die Aufsichtsbehörden von vornherein § 4 BDSG aufgrund des Anwendungsvorrangs der DS-GVO nicht angewendet.[10] Auch in anderen Zusammenhängen sind die Aufsichtsbehörden berufen, in Anwendungsfällen der Vorschriften, die Öffnungsklauseln nutzen, konkret die Vereinbarkeit mit dem Unionsrechts zu prüfen. Dabei wird die europarechtskonforme Auslegung angewendet.

Schwächer ausgestaltet sind die Aufsichtsbefugnisse zur Aufsicht über die Richtlinie 2016/680.[11] Gerade auf Bundesebene hat der Bundesbeauftragte für den Datenschutz hier nicht vollständig ausgestaltete Befugnisse.

Hervorzuheben ist § 21 BDSG, der den Aufsichtsbehörden die Befugnis zu einem Antrag auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission einräumt. Damit wird eine Anforderung des Safe-Harbor-Urteils des EuGH in innerstaatliches Recht überführt.[12] Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission, einen Beschluss über die Anerkennung von Standardschutzklauseln oder über die Allgemeingültigkeit von Angemessenheitsbeschlüssen der Kommission, von Verhaltensregeln, auf dessen Gültigkeit es für die Entscheidung der Aufsichtsbehörde ankommt für rechtswidrig, so hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen. Zuständig ist im ersten und letzten Rechtszug das Bundesverwaltungsgericht (§ 21 Abs. 3 BDSG).

Frage 2

Das Grundgesetz enthält keine ausdrückliche Regelung zum Schutz der Privatheit und ebenso wenig eine ausdrückliche Regelung zum Datenschutz. Beide Rechtspositionen sind aber infolge der Rechtsprechung insbesondere des Bundesverfassungsgerichts grundrechtlich geschützt. Zudem treffen eine Reihe von Verfassungen der Länder ausdrückliche Regelungen.

---

10 Entschließung der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 9. November 2016 (https://datenschutz-online.de).

11 Golla, Datenschutzrechtliche Schattengewächse in den Ländern – Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei, KriPoZ 4/2019 (https://kripoz.de).

12 EuGH, Urt.v.6.10.2015, C-362/14, ECLI:EU:C:2015:650, Rn. 29 - Schrems / Digital Rights Ireland.

Im Grundgesetz wird das Recht auf den Schutz des Privatlebens wie es Art. 7 GRCh beinhaltet im Schwerpunkt durch Art. 2 Abs. 1 GG geschützt.[13] Der Art. 2 Abs. 1 GG schützt alle Gehalte des Schutzes der Privatheit, die nicht in anderen Grundrechten des GG spezifisch erfasst sind und damit insbesondere den engeren Bereich persönlichen Lebens, der aber soziale Bezüge aufweisen kann.[14]

Hier ist auch das allgemeine Persönlichkeitsrecht verfassungskräftig verankert, das für die freie Entfaltung des Einzelnen ein Recht auf Respektierung eines geschützten Raums sichert.[15] Dieses Recht auf den Schutz der Persönlichkeit ist vor dem Hintergrund des Privatrechts bereits früh in der zivilrechtlichen Rechtsprechung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelt worden.[16] Dabei geht es etwa um Fallkonstellationen, in denen im Fall des Eingriffs in das Persönlichkeitsrecht durch Presseveröffentlichungen ein Ausgleich bei der Geltendmachung von Schadensersatzansprüchen geschaffen werden muss (s.u. Frage 12).[17]

Das Bundesverfassungsgericht hat aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG das Grundrecht auf informationelle Selbstbestimmung abgeleitet. Die genaue dogmatische Konstruktion wird in der Wissenschaft unterschiedlich beurteilt. Jedenfalls ist das Recht auf informationelle Selbstbestimmung eine Entfaltung von Art. 2 Abs. 1 GG. Damit hat die Judikative ein Grundrecht kreiert. Dieses Grundrecht betrifft personenbezogene Daten. Dabei hat es eine auch stark technisch orientierte Komponente, da der Datenschutz auch technische und organisatorische Maßnahmen umfasst. Dagegen schützt das allgemeine Persönlichkeitsrecht die Freiheit, das eigene Bild in der Öffentlichkeit zu gestalten. Teilweise sind die Übergänge fließend.

Der Art. 8 GRCh hat die Interpretation des innerstaatlichen Rechts bisher wenig beeinflusst zumal seine Auslegung selbst Fragen aufwirft.[18] Da seit 1983 mit dem Volkszählungs-Urteil des Bundesverfassungsgerichts das Grundrecht auf informationelle Selbstbestimmung besteht[19] und die Datenschutzgesetze dieses Grundrecht in der Folge ausgestaltet haben, war die informationelle Selbstbestimmung Kern der deutschen Rechtsprechung und Lehre zu den Fragen von Datenschutz.

13 Eingehend Schöndorf-Haubold, Das Recht auf Achtung des Privatlebens – Problemstellungen im Digitalbereich, eine rechtsvergleichende Perspektive – Deutschland (Studie für den Wissenschaftlichen Dienst des Europäischen Parlaments, abrufbar unter http://www.europarl.europa.eu/thinktank/de/home.html). S. auch Britz, Freie Entfaltung durch Selbstdarstellung, 2007.

14 Lang, in: Epping/Hillgruber (Hrsg.), Beck-OK GG, Art. 2 Rn. 41 ff.

15 BVerfGE 54, 148.

16 BGHZ 13, 334; 24, 72; 27, 284.

17 BVerfGE 101, 361.

18 Vgl. Marsch, Das europäische Datenschutzgrundrecht, 2017.

19 BVerfGE 65, 1.

B Die Annahme von materiell-rechtlichen DSGVO-Vorschriften in der nationalen Rechtsordnung

Vorbemerkung

Vor dem Wirksamwerden der Datenschutz-Grundverordnung war in der Bundesrepublik Deutschland bereits ein rechtlich ausgefeiltes System des Datenschutzes etabliert. Im Jahr 1970 hatte Hessen das erste Datenschutzgesetz der Welt, Rheinland-Pfalz dann 1973 nach Schweden das dritte. Das erste Bundesdatenschutzgesetz stammt aus dem Jahr 1977. Diese Gesetze waren noch stark informationstechnisch geprägt.[20]

Dies änderte sich mit dem Volkszählungs-Urteil des Bundesverfassungsgerichts,[21] da Datenschutz nunmehr Grundrechtsschutz ist. Denn die Konsequenz der Herausarbeitung des Grundrechts auf informationelle Selbstbestimmung ist, dass jeder staatliche Eingriff einer gesetzlichen Grundlage bedarf. In der Folge wurde seit den 80iger Jahren eine Vielzahl von Ermächtigungsgrundlagen geschaffen, um insbesondere die Erfüllung öffentlicher Aufgaben zu gewährleisten. Ein wichtiges Feld ist das Polizei- und Sicherheitsrecht.[22]

Aus der Sicht der materiellen Grundsätze hat sich daher für die Bundesrepublik Deutschland manches nur wenig geändert oder ist gar gleich geblieben, etwas im Beschäftigtendatenschutz. Die Modifikationen der Datenschutz-Grundverordnung sind wichtig, wesentlich und zukunftsweisend. Zahlreiche praktische Fragen haben sie im Hinblick auf die Ergebnisse von Einzelfällen allerdings nicht komplett umgewälzt, sondern auf eine neue Grundlage gestellt und anders akzentuiert.[23]

Frage 3

Die Grundsätze der Verarbeitung nach Treu und Glauben, der Zweckbindung und der Datenminimierung haben bereits vorher Bestand gehabt. Ihre konkreten Ausprägungen aufgrund der Datenschutz-Grundverordnung sind rechtsdogmatisch aber neu zu bewerten. Es dürfte einige Modifikationen geben, die in der deutschen Diskussion nicht immer hinreichend beachtet werden, weil die Beharrungskraft eingeschliffener datenschutzrechtlicher Lösungen stark ist. Dies betrifft etwa die Datenminimierung, die an die Stelle der Datensparsamkeit tritt. Damit könnten Änderungen verbunden sein, die aber oft nicht wahrgenommen werden. Auch Zweckbindung und insbesondere Zweckänderung nach Art. 6 Abs. 4 DS-GVO zeigen bei genauer Lektüre andere Ausprägungen, als sie das vorherige Recht kannte.

20 Schulte, Vom quantitativen zum qualitativen Datenschutz, 2018, S. 60 ff.
21 BVerfGE 65, 1.
22 Dazu Zaremba, Die Entwicklung polizeirelevanter datenschutzrechtlicher Bestimmungen, 2014.
23 Roßnagel, Das neue Datenschutzrecht, 1. Aufl. 2018.

Diese rechtsdogmatischen Feinheiten haben bisher in der Praxis noch keine Rolle gespielt. Die nationalen Aufsichtsbehörden wenden die Grundsätze auf der Grundlage der DS-GVO an und in einer Vielzahl von Fällen sind die kleineren Modifikationen ohne praktische Auswirkung. Die Rechtsprechung hat bisher nur selten zu den Neuregelungen Stellung nehmen können.

Frage 4

Da in der Bundesrepublik Deutschland Datenschutz traditionell als das Grundrecht auf informationelle Selbstbestimmung verstanden wird, hat die Einwilligung als Ausdruck der freien Entscheidung über die Selbstbestimmung wesentlichen Einfluss.[24] Diese Rolle erscheint an mancher Stelle übergewichtet angesichts der Realitäten der Digitalwirtschaft, in der eine freiwillige und informierte Einwilligung oftmals schwer zu erteilen ist.[25] Rechtsprechung und Lehre halten aber überwiegend an der zentralen Rolle der Einwilligung fest.[26] Sie erfordert die Festlegung des Zwecks der Verarbeitung und die Information der betroffenen Person, weil sie nur dann freiwillig und informiert i.S.d. Art. 4 Nr. 11 DS-GVO abgegeben werden kann.[27]

Zunächst ist der Vertrag oder die Einwilligung als Rechtsgrundlage vorrangig zu prüfen (Art. 6 Abs. 1 lit. a und b DS-GVO). Berechtigte Interessen kommen ergänzend zum Tragen. Denn die Einwilligung legt die Verfügungsmacht in die Hände des Betroffenen, das berechtigte Interesse bestimmt dagegen der Verantwortliche.

Die Rechtsgrundlage der berechtigten Interessen wird von den Aufsichtsbehörden konzeptionell eher eng gesehen. Allerdings hat sich in der Praxis erwiesen, dass es eine Vielzahl von Anwendungsfällen gibt. Es handelt sich aber bei Art. 6 Abs. 1 lit. f DS-GVO nicht um einen Auffangtatbestand, da sonst ein Anreiz dafür geschaffen wird, alle möglichen Datenverarbeitungen auf die berechtigten Interessen zu stützen. Die Leitlinien 2/2019 des Europäischen Datenschutzausschusses halten diese Grundsätze fest.[28]

Die berechtigten Interessen spielen in der Praxis allerdings gerade im Bereich der Dienstleistungen und Inhalte, die im Internet angeboten werden, also in der Plattformökonomie eine erhebliche Rolle. Die in Erwägungsrund 47 der DS-GVO eröffnete

24 Schantz, in: Simitis/Hornung/Spiecker gen Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 6 Abs. 1 DSGVO, Rn. 3.

25 Kritisch Krönke, Der Staat 2016, 319; Veil, NJW 2018, 3337 (3344).

26 Buchner/Kühling, DuD 2017, 544; Heberlein, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 6 Rn. 5; Schantz, in: Simitis/Hornung/Spiecker gen Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 6 Abs. 1 DSGVO, Rn. 3.

27 Schwartmann/Klein, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 6 Rn. 13f.

28 Guidelines 2/2019, (https://edpb.europa.eu).

Möglichkeit, Direktwerbung auf die Grundlage der berechtigten Interessen zu stützen, ist anerkannt.

Jedoch ist mangels einer ePrivacy-Verordnung der Verantwortliche verpflichtet, die Einwilligung etwa bei dem Einsatz von TrackingTools einzuholen. Da die ePrivacy-Verordnung noch nicht existiert, gilt die DS-GVO für soziale Netzwerke und Telemedien direkt.[29] Die deutsche Datenschutzkonferenz (DSK) hat in einem Positionspapier vom 29. März 2019 festgehalten, dass daher grundsätzlich Einwilligungen für Maßnahmen des Tracking erforderlich sind und diese nur in Ausnahmefällen auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden können.

Im Fall der Rechtsgrundlage Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) besteht ein besonderer Schutzmechanismus für die Verfügungsmacht des Einzelnen über seine Daten. Die Regelung des Art. 7 Abs. 4 DS-GVO wird als Kopplungsverbot mit begrenzter Reichweite verstanden.[30] Ein striktes Kopplungsverbot ist der Vorschrift wohl nicht zu entnehmen. Die Freiwilligkeit der Einwilligung muss aber gewährleistet sein, auch dann, wenn weitere vertragliche Pflichten daran hängen.[31]

Bei allen weiteren Rechtsgrundlagen ist der rechtliche Anknüpfungspunkt für die Ausübung der Verfügungsmacht über die eigenen Daten der Grundsatz der Erforderlichkeit.[32] Die Erforderlichkeit nach Art. 6 Abs. 1 lit. b ff. DS-GVO ist ein Standardinstrument des Datenschutzrechts. Datenverarbeitungen sind dann rechtmäßig, wenn sie erforderlich sind. Dieser allgemeine Grundsatz wird konkret in unterschiedlichen rechtlichen Situationen relevant. Die Erforderlichkeit steht in engem Zusammenhang mit der Zweckbindung und der Datenminimierung. Nur die Verarbeitung personenbezogener Daten, die für die Vertragserfüllung wirklich erforderlich sind, ist zulässig, darüber hinaus dürfen die Daten nicht verarbeitet werden. Bei vertraglichen Beziehungen, die der Datenverarbeitung zugrunde liegen (Art. 6 Abs. 1 lit. b DS-GVO) führt dies zu einer Bindung der Reichweite der Datenverarbeitung an den Vertragszweck. Dabei wird überwiegend die Erforderlichkeit in einem weiten Sinne auf die Durchführung des gesamten Vertrages und nicht nur auf eine konkrete Erfüllungshandlung bezogen.[33]

Die Interessenabwägung zwischen dem Interesse des Verantwortlichen an der Datenverarbeitung und den Rechten und Freiheiten der betroffenen Person spielt eine zentrale Rolle auch bei der Datenverarbeitung durch öffentliche Stellen. Das

29 Richter, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 95 Rn. 8 ff.

30 Golland, MMR 2018, 130; Heberlein, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 7 Rn. 53.

31 Kugelmann, DuD 2016, 566 (567).

32 Reimer, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Auflage 2018, Art. 6 Rn. 12.

33 Petri, in Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Auflage 2018, Art. 6 Rn. 42; Schwartmann/Klein, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 6 Rn. 49.

Bundesverwaltungsgericht hat entschieden, dass auf den presserechtlichen Auskunftsanspruch nach innerstaatlichem Landesmediengesetz, das auf der Grundlage von Art. 6 Abs. 1 lit. e i.V.m. Abs. 3 DS-GVO beruht, der Art. 6 Abs. 1 lit f. DS-GVO zwar nicht unmittelbar anwendbar ist, aber seine Maßstäbe der Abwägung übertragbar sind.[34]

Frage 5

Die Thematik der Daten als Gegenleistung für Datenverarbeitungen wird in Deutschland umfangreich und intensiv diskutiert. Diese Diskussion wird unter verschiedenen Vorzeichen geführt. Zum einen wird der Begriff der Datensouveränität gebraucht, der allerdings schillernd ist. Souverän kann hier der Einzelne sein, indem er über seine Daten selbst bestimmt. Souverän kann aber auch der Datenverarbeiter, also der Verantwortliche sein, indem er berechtigte Interessen festlegt. Das Zivilrecht wird darauf geprüft, ob und inwieweit es Ansatzpunkte für eine Bewältigung der Fragen bietet, die aus dem Charakter der Daten als Gegenleistung entstehen und ob andere Vertragstypen erforderlich sind.[35]

Eine insbesondere wirtschaftsrechtlich geführte Diskussion dreht sich um den Begriff des Dateneigentums.[36] Es wird behauptet, man könne Eigentum an Daten haben, das dann auch zivilrechtlichen Regelungen unterfallen soll, die an Regelungen des Eigentums angelehnt sind. Dabei wird verkannt, dass personenbezogene Daten eigenen Charakter aufweisen, der mit einem ausschließlichen und absoluten Eigentumsrecht nicht einzufangen ist. Diese Debatte geht aber weiter.

Die werbetreibende Wirtschaft versucht, den Begriff des Dateneigentums und die Frage, bezahlen mit Daten, zu akzentuieren. Hier geht es um eine Ausweitung der Verfügungsmöglichkeiten über personenbezogene Daten durch die Verantwortlichen. Aus zivilrechtlicher Sicht ist die Frage der Einwilligung von großer Bedeutung, da es hier auch um Vertragsabschlüsse geht. Die Widerruflichkeit der Einwilligung ist für den Bestand von zivilrechtlichen Beziehungen nicht unproblematisch. Daher wird teilweise angezweifelt, ob diese Widerrufbarkeit tragfähig ist. Aus datenschutzrechtlicher Sicht ist die Rechtslage allerdings klar, da die Einwilligung widerrufbar sein muss, um der Freiheitsausübung Rechnung tragen zu können.

Auch auf politischer Ebene gab es Diskussionen um die Verwendung von personenbezogenen Daten als Gegenleistung für die Bereitstellung von digitalen Inhalten. Es wurde vorgeschlagen, einen freien Zugang zu Daten zu ermöglichen, also Verantwortliche dazu zu verpflichten, bei ihnen vorhandene Daten öffentlich zugänglich

34 BVerwG, Urt.v.27.09.2018, Az. 7 C 5.17, DVBl. 2019, 765.

35 Specht, JZ 2017, 763.

36 S. die Beiträge in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, 2019; Jöns, Daten als Handelsware (DIVSI), 2016.

zu machen (open access – „Daten für alle"). Dies zielte nicht zuletzt auf Google oder facebook, die dann ihren Datenschatz zugänglich machen müssten. Diese politischen Bestrebungen haben bisher keine konkreten Folgen gezeitigt.

Frage 6

In der Bundesrepublik Deutschland wurde auf der Grundlage des Art. 22 Abs. 2 lit. b BDSG insbesondere die Vorschrift des § 37 BDSG geschaffen.[37] Die Regelung erlaubt Ausnahmen bei Versicherungsverträgen. Erfolgt die Leistungserbringung in dessen Rahmen, kann eine Entscheidung ausschließlich auf automatisierte Entscheidung gestützt werden. Voraussetzung ist, dass entweder dem Begehren der betroffenen Person stattgegeben wurde (§ 37 Abs. 1 Nr. 1 BDSG) oder verbindliche Entgeltvorschriften im Hinblick auf Heilbehandlungen bestehen, die dem Betroffenen weitere Schutzrechte einräumen (§ 37 Abs. 1 Nr. 2 BDSG). Ziel ist die reibungslose Abwicklung von Massenverfahren, deren Abwicklung im Interesse der Person liegt, die bereits einen entsprechenden Vertrag geschlossen hat.[38]

Frage 7

Die betroffene Person hat ein subjektives Recht auf Löschung, wenn die Daten für die Erreichung der Zwecke, zu denen sie erhoben oder verarbeitet werden, nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a DS-GVO).[39] Ist die Speicherung nicht mehr erforderlich, sind die Daten zu löschen, um damit auch dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und dem Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) Rechnung zu tragen. Anknüpfungspunkt für die Verpflichtung des Verantwortlichen zur Löschung ist der im deutschen Datenschutzrecht schon immer zentrale Grundsatz der Erforderlichkeit der Datenverarbeitung (s. Art. 6 Abs. 1 lit. b, c, d, e, f DS-GVO). Daher ist das Recht auf Löschung schon seit langem ein wesentliches Element des deutschen Datenschutzrechts. Nach § 35 BDSG und ähnlichen Regelungen des innerstaatlichen Rechts ist das Recht auf Löschung beschränkt, wenn die Löschung unverhältnismäßig hohen Aufwand bedeuten würde und weitere Voraussetzungen vorliegen.

37 Atzert, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 22 Rn. 76.

38 Paschke/Scheurer, in: Gola/Heckmann (Hrsg.), BDSG, 13. Aufl. 2019, § 37 Rn. 2.

39 Leutheusser-Schnarrenberger, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Aufl. 2018, Art. 17 Rn. 18.

Die Datenschutzaufsichtsbehörden verlangen grundsätzlich von den Verantwortlichen Löschungskonzepte. Solche Konzepte bestehen allerdings eher selten. Im Kern geht es um ein Datenschutzmanagement, das der Frage Rechnung trägt, wie lange man die personenbezogenen Daten benötigt.

Löschfristen können nur im Hinblick auf einzelne Situationen der Datenverarbeitung zu bestimmen. Dem Grunde nach ist dann zu löschen, wenn die Datenverarbeitung nicht mehr erforderlich ist. Dies kann im Privatrechtsverkehr sehr unterschiedliche Zeitdauern betreffen. Hier ist angesichts der Vielfalt der Situationen, in denen verarbeitete Daten gelöscht werden sollten oder müssten, keine abstrakte Vorgabe ersichtlich. Die Datenschutzaufsichtsbehörden arbeiten an der Bewertung von Einzelfällen. Allgemeine Richtlinien werden nicht erlassen.

In der Verarbeitungssituation der Videoüberwachung vertreten die Datenschutzaufsichtsbehörden grundsätzlich eine Löschungspflicht nach 72 Stunden. Wird also eine zulässige Videoüberwachung durchgeführt, etwa im öffentlichen Personennahverkehr, sind die Aufnahmen spätestens nach 72 Stunden zu löschen, wenn sich keine Anhaltspunkte ergeben, die eine weitere Speicherung erlauben. Gleiches gilt etwa für Videoüberwachung in Einkaufszentren oder Kaufhäusern.

Die Löschungspflichten staatlicher Stellen werden teils strenger gehandhabt als für private Stellen. Dies gilt etwa für die Aufzeichnung personenbezogener Daten durch die Polizei. Dies erfolgt zwar auf der Rechtsgrundlage der Richtlinie 2016/680, folgt aber ähnlichen Maßgaben. Hier bedarf es der Prüfung, wie lange die Speicherung erforderlich ist.

Das Recht auf Löschung wird begleitet durch die Notwendigkeit der Dokumentation. In diesem Umfeld spielen technische und organisatorische Maßnahmen nach Art. 24, 32 DS-GVO eine große Rolle. Wenn Daten nicht gelöscht werden, muss dokumentiert werden, warum ihre weitere Speicherung für erforderlich gehalten wird.

Wenn ein Einzelner sein subjektives Recht auf Löschung nach Art. 17 DS-GVO geltend macht, wird in diesem Fall geprüft, ob den allgemeinen Maßgaben Rechnung getragen wurde. Das Recht auf Löschung wird allerdings deutlich seltener geltend gemacht als das Recht auf Auskunft.

Nach der Entscheidung des EuGH im Fall Google/Spain[40] haben die Niederlassungen der Betreiber von Suchmaschinen in der Bundesrepublik Deutschland überwiegend Mechanismen eingerichtet, um das Recht auf Vergessenwerden zu verwirklichen. So hat Google ein Verfahren etabliert und berichtet öffentlich über Löschungsverfahren und Löschungsentscheidungen.[41]

---

40 EuGH, C-131/12, ECLI:EU:C:2014:317 - Google/Spain; dazu Nolte, NJW 2014, 2238.

41 Leutheusser-Schnarrenberger, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Aufl. 2018, Art. 17 Rn. 66.

Frage 8

In der Bundesrepublik Deutschland wurde in großem Maße von der Möglichkeit nach Art. 85 DS-GVO, im Medienbereich spezifisches innerstaatliches Recht zu erlassen, Gebrauch gemacht. Dies liegt daran, dass Medien und Kultur zu den Gesetzgebungszuständigkeiten der Länder zählen. Daher wurden die Landesmediengesetze jeweils angepasst. Die Medien- oder Pressegesetze der Länder enthalten nunmehr Regelungen zur Wahrnehmung des Datenschutzes. Im Mittelpunkt der Diskussion steht dabei die Frage der Kontrolle. Im Schwerpunkt wird auf die Selbstkontrolle der Medien gesetzt. Dies unterliegt durchaus Zweifeln angesichts der Regelung des Art. 85 DS-GVO. Die Länder haben dabei unterschiedliche Kontrollsysteme etabliert. Die Einbeziehung der staatlichen Datenschutzaufsichtsbehörde des jeweiligen Landes ist dabei der entscheidende Punkt, da jeder Anschein von Zensurmöglichkeiten vermieden werden soll.[42]

Für die audiovisuellen Medien wird in der Bundesrepublik Deutschland die Rechtsgrundlage Staatsvertrag gewählt. Alle Länder haben gemeinsam Staatsverträge geschlossen, die den Rundfunk regeln.[43] Der Rundfunkstaatsvertrag enthält Regelungen für die Datenschutzbeauftragten der Rundfunkanstalten. Der Rundfunkstaatsvertrag ist begleitet von einem Staatsvertrag zu der Frage, wie die Finanzierung des Rundfunks geregelt wird.[44] Dieser Rundfunkbeitragsstaatsvertrag enthält auch die Regelung, dass die Haushaltsabgabe, die neu eingeführt wurde, im Rahmen eines Meldedatenabgleiches festgestellt werden kann. Die auf der Grundlage des Rundfunkbeitragsstaatsvertrages etablierte Einrichtung, der Beitragsservice, hat also Rechte gegenüber den staatlichen Meldebehörden, um festzustellen, welche Personen in welcher Wohnung gemeldet sind. Im Kern geht es darum, dass jeder Haushalt verpflichtet ist, die Rundfunkabgabe zu zahlen. Diesen Rundfunkbeitrag festzustellen ist das ausschlaggebende Problem. In der nunmehr für 2020 geplanten Neufassung des Rundfunkbeitragsstaatsvertrages wird alle vier Jahre ein umfassender Meldedatenabgleich erlaubt. Damit können die Beiträge für den öffentlich-rechtlichen Rundfunk gerecht ermittelt werden, da auch Personen, die sich nicht freiwillig beim Beitragsservice der Rundfunkanstalten melden, entdeckt werden können. Allerdings sind dies in der Relation nur wenige Personen. Die Datenschutzaufsichtsbehörden halten einen vollständigen Meldedatenabgleich der Gesamtbevölkerung für diesen Zweck für verfassungsrechtlich zweifelhaft, weil er

42 Dazu mit pressefreundlicher Ausrichtung Cornils, ZUM 2018, 561 und ders., Das datenschutzrechtliche Medienprivileg unter Behördenaufsicht? Der unionsrechtliche Rahmen für die Anpassung der medienrechtlichen Bereichsausnahmen (in § 9c, § 57 RStV-E und den Landespressegesetzen) an die EU-Datenschutz-Grundverordnung, Tübingen, 2018.

43 Vgl. BVerfGE 136, 9, Rn. 44 ff. – ZDF-Fernsehrat; s. BVerfGE 73, 118 zum dualen System.

44 BVerfGE, Urteil vom 18.07. 2018, 1 BvR 1675/16, 1 BvR 745/17, 1 BvR 836/17, 1 BvR 981/17 - Rundfunkbeitrag.

ernsthaften Bedenken im Hinblick auf die Verhältnismäßigkeit des Eingriffes in das Grundrecht auf informationelle Selbstbestimmung begegnet.

C Nationale Durchsetzung von Datenschutzrecht

Frage 9

Die Datenschutzaufsichtsbehörden des Bundes und der Länder in der Bundesrepublik Deutschland sind auf der Grundlage ihres jeweiligen Bundes- oder Landesgesetzes errichtet. Die Aufgaben und Befugnisse folgen unmittelbar aus Art. 57, 58 DS-GVO.[45] Soweit der private Bereich betroffen ist, gibt es keine darüber hinausgehenden Befugnisse. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist in §§ 8 ff. BDSG geregelt. Die Mehrzahl der Landesbeauftragten für den Datenschutz sind zugleich auch Beauftragte für die Informationsfreiheit nach dem jeweiligen Landesinformationsfreiheits- oder Landestransparenzgesetz.[46] In drei Ländern der Bundesrepublik gibt es bisher kein entsprechendes Informationsfreiheitsrecht (Bayern, Niedersachsen, Sachsen), dort sind die Landesbeauftragten nur für den Datenschutz zuständig.

Die Datenschutzaufsichtsbehörden in der Bundesrepublik Deutschland sind regelmäßig oberste Bundes- oder Landesbehörden (z.B. § 8 Abs. 1 S. 1 BDSG). Derart wird die Konsequenz aus der Unabhängigkeit gezogen, die der EuGH fordert.[47] Der oder die Beauftragte wird vom jeweiligen Parlament gewählt (z.B. § 11 BDSG). Der Bundestag oder die Landtage legen also die Behördenspitze durch Wahl fest. Die weitere Zusammensetzung der Behörde erfolgt nach allgemeinen Regeln des öffentlichen Dienstrechtes. Die Personalhoheit obliegt der oder dem Beauftragten.[48] Maßgeblich für die Personalstärke der Behörde ist der jeweilige Haushalt. Die Regelung des Art. 52 Abs. 6 DS-GVO wird in den Ländern und im Bund unterschiedlich konkretisiert. Hier besteht eine indirekte Möglichkeit der Einflussnahme, indem das jeweilige Parlament Stellen bewilligt oder nicht. Dies hat konkrete Auswirkungen auf die Arbeitsfähigkeit der Behörde und die Möglichkeit, Aufgaben wahrzunehmen. Umgekehrt ist aufgrund der beschränkten Personalausstattung eine Prioritätensetzung durch die Behörde selbst regelmäßig unabweisbar. Der von den Beauftragten vorgetragene Mehrbedarf an Personal zur Verwirklichung der DS-GVO

45 Kugelmann, ZD 2020 (Heft 2), Ziff. III.

46 Kritisch zu dieser Personalunion Ibler, in: Festschrift Peine, 2016, S. 457.

47 EuGH Urt.v.9.3.2010, C-518/07, ECLI:EU:C:2010:125 - Kommission/Deutschland; EuGH Urt.v.16.10.2012, C-614/10, ECLI:EU:C:2012:631 – Kommission/Österreich; EuGH Urt.v.8.4.2014, C-288/12, ECLI:EU:C:2014:237 - Kommission/Ungarn.

48 Kugelmann, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 52 Rn. 44.

wurde im Bund und den Ländern in sehr unterschiedlichem Ausmaß vom Haushaltsgesetzgeber aufgegriffen.[49]

Die besondere Situation der Wahrnehmung von Grundrechten durch eine unabhängige Stelle erfordert spezifische Regelungen für die unabhängigen Stellen. Dies stellt Art. 8 Abs. 3 GRCh klar. Konsequenz ist, dass eine Aufsicht im hergebrachten Sinne über die Datenschutzbeauftragten unzulässig ist. Dies folgt auch aus Art. 52 Abs. 1 und 2 DS-GVO.[50] Aus dem deutschen Verfassungsrecht wird grundsätzlich die Vorgabe abgeleitet, dass Behörden, die Eingriffsverwaltung durchführen, einer Aufsicht unterliegen sollen, um insbesondere die demokratische Legitimation des Verwaltungshandelns sicherzustellen.[51] Dies wurde von der Bundesregierung in dem Verfahren C-518/07 auch im Hinblick auf die Datenschutzbeauftragten vorgetragen, aber vom EuGH zurückgewiesen.[52]

In der konkreten Rechtspraxis und in den Regelungen der Bundes- und Landesdatenschutzgesetze stellt sich die Situation differenziert dar. Hier werden praktische Möglichkeiten der Einflussnahme durchaus sichtbar. Ob und inwieweit diese Situation mit den Regelungen der Datenschutz-Grundverordnung vollständig vereinbar ist, begegnet Bedenken, da auch indirekte Einflussnahmen nach der Rechtsprechung des EuGH unzulässig sind.[53] Die Diskussion führt in die Gemengelage zwischen Unionsrecht und innerstaatlichem Verfassungsrecht. Zweifel wirft etwa die Frage der Aufsicht über den Beauftragten auf.[54] Einige Landesdatenschutzgesetze sehen eine Dienstaufsicht vor (§ 14 Abs. 1 Satz 2 LDSG Rheinland-Pfalz).[55] Teils ist dies auch in den Landesverfassungen angedeutet. Trotz des Anwendungsvorrangs des Unionsrechts sind hier die Spielräume zu beachten, die das innerstaatliche Verfassungsrecht noch ausnutzen kann. Daher kann eine generelle Beurteilung sämtlicher Regelungen nicht pauschal erfolgen. Allerdings ist auch festzustellen, dass es in der Praxis fast nie Probleme gibt. Die Datenschutzbeauftragten sind aufgrund ihrer Wahl und ihrer unabhängigen Stellung in einer herausgehobenen Position, die allgemein von der Politik auch anerkannt wird.

---

49 Zum Ganzen Roßnagel, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017.

50 Kugelmann, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 52 Rn. 17.

51 Eingehend Thomé, Reform der Datenschutzaufsicht, 2015, insbesondere S. 107 ff.; vgl. Wolff, ThürVBl. 2015, 205 (209) f. zu einem parlamentarischen Untersuchungsausschuss über das Vorgehen eines Landesdatenschutzbeauftragten.

52 EuGH Urt.v.9.3.2010, C-518/07, ECLI:EU:C:2010:125 - Kommission/Deutschland, Rn. 25.

53 Kugelmann, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 52 Rn. 37.

54 Thomé, Reform der Datenschutzaufsicht, 2015, S. 123.

55 Für zulässig hält dies Glauben, DVBl. 2017, 488; für unzulässig Boehm, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Auflage 2018, Art. 52 Rn. 25; Nguyen, in: Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 52 Rn. 12.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder arbeiten in der Datenschutzkonferenz zusammen.[56] In regelmäßigen Konferenzen werden gemeinsame Positionen festgelegt, um die Rechte der Betroffenen zu schützen und den Verantwortlichen Hilfestellung in der Anwendung zu geben. Dies betrifft konkrete Orientierungshilfen zu bestimmten Themen. Es betrifft Positionspapiere zur Handhabung rechtlicher Regelungen. Die Datenschutzkonferenz trifft Entschließungen zu datenpolitischen Fragen. Sie hat etwa Kurzpapiere zur Auslegung der Datenschutz-Grundverordnung geschaffen. Jeder und jede Datenschutzbeauftragte ist unabhängig. Damit kann es sein, dass in einem Land der Bundesrepublik Deutschland vereinzelt andere Handhabungen Bestehen als in einem anderen Land.

Alle Datenschutzbeauftragten in der Bundesrepublik Deutschland sind sowohl für Datenverarbeitung durch private wie durch öffentliche Stellen zuständig (vgl. z.B. § 1 BDSG). Die Zuständigkeiten für den öffentlichen Bereich umfassen auch Polizei und Justiz im Sinne der Richtlinie 2016/680.

Im Anwendungsbereich der DS-GVO verfügen die Beauftragten über alle Befugnisse des Art. 58 DS-GVO (vgl. deklaratorisch § 16 Abs. 1 S. 1 BDSG). Gegenüber öffentlichen Stellen besteht allerdings keine Möglichkeit, Geldbußen zu verhängen. Als zusätzliche Maßnahme ist die Beanstandung vorgesehen (§ 16 Abs. 2 BDSG). Das hergebrachte Instrument der Beanstandung eines Datenschutzverstoßes wird aus dem vorherigen Recht fortgeschrieben. Dabei handelt es sich um eine Maßnahme, die einer Verwarnung gegenüber privaten Stellen ähnelt. Der Datenschutzverstoß wird festgestellt und die weitere Verarbeitung von Daten wird auf rechtmäßiger Basis angemahnt und daraufhin kontrolliert. Die zuständige Rechtsaufsicht wird informiert und prüft die Einhaltung der Vorgaben.[57]

Für die Datenverarbeitung privater Stellen sind die Landesbeauftragten zuständig. Der Bundesbeauftragte hat lediglich beschränkte Zuständigkeiten für Unternehmen der Telekommunikation, also etwa für die Deutsche Telekom und die Post (§ 115 Abs. 4 TKG, § 42 Abs. 3 PostG). Die Aufsicht und Kontrolle über die private Wirtschaft obliegt den Landesbeauftragten. Dies hält § 40 BDSG fest.[58]

Die Rechtsdurchsetzungsbilanz fällt dem Grunde nach deshalb positiv aus, weil insbesondere Verwarnungen und auch Geldbußen erfolgt sind. Die Mehrzahl der Fälle trägt innerstaatlichen Charakter. Dies betrifft etwa Fälle der Videoüberwachung oder der Falschübermittlung von Daten in geringem Umfang. Folglich bewegt sich die überwiegende Zahl der Geldbußen im 3- oder 4stelligem Bereich.

Die deutschen Datenschutzaufsichtsbehörden sind sich ihrer Verantwortung für die Rechtsdurchsetzung bewusst. Angesichts der beschriebenen längeren Dauer und der

56 S. http://www.datenschutzkonferenz-online.de.
57 Wieczorek, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Auflage 2018, § 16 BDSG Rn. 15.
58 Dix, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Auflage 2018, § 40 BDSG Rn. 1.

rechtsstaatlichen Anforderungen an die Verfahren sind die Maßnahmen auf der Grundlage der DS-GVO erst langsam in Gang gekommen. Sie können nur Verstöße betreffen, die unter der Geltung der DS-GVO, also seit dem 25. Mai 2018, vorgekommen sind. Diese Verstöße werden durch Beschwerden von Individuen oder auf anderem Wege etwa durch die Meldung von Datenschutzverletzungen nach Art. 33 DS-GVO oder durch Hinweise des Datenschutzaufsichtsbehörden bekannt. Sodann treffen diese Ermittlungsmaßnahmen. Das Verfahren beginnt regelmäßig mit den Informationsersuchen gegenüber dem Verantwortlichen, damit Stellung gegenüber dem Vorwurf genommen werden kann. Diese Verfahren sind teils langwierig. Dies betrifft gerade auch die Geldbußen. Hier ist nach bundesdeutscher Rechtslage das Ordnungswidrigkeitengesetz (OWiG) einschlägig. Die Feststellung des Verstoßes kann mit einer Geldbuße nach Art. 83 DS-GVO geahndet werden. Das Verfahren erfolgt aber nach dem Ordnungswidrigkeitengesetz und unterliegt den einschlägigen Regelungen. Einige Regelungen des Ordnungswidrigkeitengesetzes kommen aufgrund des Anwendungsvorrangs des Unionsrechts nicht zum Zuge. Dies betrifft nach zutreffender Auffassung etwa die §§ 30, 130 OWiG mit der Folge, dass nicht nur Organisationsverschulden zugerechnet werden kann, sondern auch das Verhängen einer Geldbuße gegenüber einer juristischen Person zulässig ist.[59]

Frage 10

Rechtliche Einschränkungen, die der Strategie von Behandlungen von Beschwerden auferlegt wurden, sind nicht ersichtlich. Sie wären auch schwerlich mit Art. 78 DS-GVO zu vereinbaren. Indirekte Folgewirkungen haben die Präzisierung von Anwendungsbereichen oder die Einschränkung von Betroffenenrechten auf der Grundlage des Art. 23 DS-GVO. Das Recht auf Beschwerde ist ansonsten abschließend in der DS-GVO geregelt.

Die deutschen Aufsichtsbehörden haben im Jahr 2018 nach Inkrafttreten und Wirksamwerden der Datenschutz-Grundverordnung einen Schwerpunkt auf die Behandlung von Beschwerden gelegt. Grund dafür ist, dass nach Art. 78 Abs. 2 DS-GVO jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn nicht die zuständige Aufsichtsbehörde sich innerhalb von drei Monaten mit der Beschwerde befasst. Aufgrund dieser Dreimonatsfrist ist die Behandlung von Beschwerden durchgehend als Priorität gesehen worden. Die Beschwerde drückt die individuelle Freiheitsgestaltung des einzelnen Beschwerdeführers aus, der sich in seinen Rechten aus

59 Brodowski/Nowak, in: Wolff/Brink (Hrsg.), Beck-OK (28. Edition), § 41 BDSG Rn. 11 ff. m.w.N. auch zur Gegenauffassung.

dem Datenschutzrecht verletzt fühlt. Auch angesichts der Verknüpfung mit der grundrechtlichen Gewährleistung ist die Beschwerde nach wie vor als Priorität einzustufen.

Jenseits von der Festlegung proaktiver Strategien stand zunächst die Umstellung auf die Beschwerden nach der DS-GVO und ihre Bewältigung im Vordergrund. Dies hat zu organisatorischen und verfahrensmäßigen Konsequenzen geführt. Die Behörden haben sich intern so organisiert, dass sie eine angemessene Behandlung der Beschwerden gewährleisten können. Dies betrifft insbesondere auch die Erörterung von Beschwerden mit grenzüberschreitendem Bezug. Denn im Falle grenzüberschreitender Verarbeitungen oder erheblicher Beeinträchtigung im Sinne des Art. 56 Abs. 1 und 2 DS-GVO ist die Zuständigkeit festzustellen. Dann greift der Mechanismus der Datenschutz-Grundverordnung, dass eine federführende Aufsichtsbehörde das Verfahren zentral führen soll. Zu diesem Zweck ist eine Online-Plattform etabliert worden, die eine schnelle und reibungslose Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden ermöglichen soll. Diese IMI-Plattform hatte Anlaufschwierigkeiten, da zunächst die Rahmenbedingungen ihrer Nutzung und die konkrete Handhabung der verschiedenen Möglichkeiten auf europäischer Ebene geklärt werden mussten. Dies hat die Behandlung von Beschwerden zunächst etwas kompliziert gemacht. Inzwischen ist mit einer Arbeitsgruppe und weiteren verfahrensmäßigen Hilfestellungen der Zustand verbessert worden. Dennoch bleibt die weitere Optimierung dieser Plattform eine Daueraufgabe.

Einschränkungen der Behandlung von Beschwerden liegen in den vorhandenen Ressourcen. Die deutschen Datenschutzaufsichtsbehörden sind teilweise im Personal aufgestockt worden. Zum einen betrifft dies aber nicht alle, zum anderen ist die Last der Behandlung von Beschwerden auch mit dem erweiterten Personalstock kaum angemessen zu bewältigen.

Angesichts der begrenzten Ressourcen in den Datenschutzaufsichtsbehörden sind jeweils Weichenstellungen vorgenommen worden, um dem enorm gestiegenen Arbeitsanfall Rechnung zu tragen. In der Bundesrepublik Deutschland hat sich diese Abstimmung teilweise auf der Ebene der Datenschutzkonferenz abgespielt. Die unabhängigen Aufsichtsbehörden des Bundes und der Länder sind in der Datenschutzkonferenz zusammengeschlossen, um gemeinsame Linien zu finden. Im 2. Halbjahr 2018 und auch noch zu Beginn des Jahres 2019 betrafen die Weichenstellungen u.a. auch die Frage der Behandlung von Beschwerden. Beispiele sind die innerstaatliche Abgabe oder das Verständnis von nicht grenzüberschreitenden Fällen gem. Art. 56 Abs. 2 DS-GVO. Die innerstaatliche Abgabe betrifft die Zusammenarbeit der deutschen Behörden. Hier wird analog der europäischen Vorgabe des Art. 56 Abs. 1 DS-GVO auf die Hauptniederlassung abgehoben. Beschwerden gegenüber einem Unternehmen mit Sitz in Nordrhein-Westfalen werden dann an die nordrhein-westfälische Datenschutzaufsichtsbehörde abgegeben. Einzelheiten sind hier streitig, etwa die Frage, ob und von wem die Benachrichtigung des

Betroffenen über die Abgabe erfolgt. In der Zwischenzeit konnten hier handhabbare Kompromisse in der DSK erzielt werden.

Die Bewertung als grenzüberschreitend oder nicht grenzüberschreitend und die Bewertung eines Falles als lokal begrenzt sind wichtige und ausschlaggebende Fragen in der täglichen Behördenarbeit.[60] Die Auslegung des Verständnis des Art. 56 Abs. 1 und 2 DS-GVO sollen vom Europäischen Datenschutzausschuss in einschlägigen Handreichungen konkretisiert werden. Die konkrete Vorgehensweise der europäischen Datenschutzaufsichtsbehörden unterscheidet sich im Detail durchaus noch. Dies kann Auswirkungen auf den Einzelfall haben, etwa im Fall unterschiedlicher Bewertungen konkreter Verarbeitungen als lokal begrenzt. Teilweise finden hier auch bilaterale Kontakte der jeweiligen Behörde mit der grundsätzlich federführenden Behörde für das verantwortliche Unternehmen statt. Beschwerden gegen Facebook, Google oder Amazon sind Massenphänomene, die daher auf europäischer Ebene besonders Berücksichtigung in der Bearbeitung von Beschwerden finden.

Frage 11

Das BDSG und die Landesdatenschutzgesetze enthalten eigene strafrechtliche Tatbestände und nutzen damit Art. 84 DS-GVO.[61] Nach § 42 Abs. 1 BDSG wird mit Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe bestraft, wer Daten wissentlich an Dritte übermittelt und gewerbsmäßig handelt. Mit Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe wird gemäß § 42 Abs. 2 BDSG bestraft, wer unberechtigt Daten verarbeitet und gegen Entgelt oder mit Schädigungsabsicht handelt. Sanktionen des Strafrechts für etwa das Ausspähen von Daten gem. § 202 a Strafgesetzbuch sind hiervon unabhängig.

Andere verwaltungsrechtliche Sanktionen im Sinne des Art. 84 DS-GVO bestehen in der Bundesrepublik Deutschland nicht. Die breit gefächerten Befugnisse des Art. 58 DS-GVO und die Regelung des Art. 83 DS-GVO zu den Geldbußen werden insofern als ausreichend erachtet.

Die deutschen Datenschutzaufsichtsbehörden machen von den Abhilfebefugnissen in unterschiedlichem Ausmaß gebrauch. Ein Schwerpunkt liegt bei dem Instrument der Verwarnung. In der Vergangenheit liegende Verstöße gegen das Datenschutzrecht können nach Art. 58 Abs. 2 lit. b DS-GVO damit angemessen geahndet werden.[62] Angesichts der durchaus aufwändigen Verwaltungsverfahren, um Verwaltungsakte oder auch Geldbußen

60 Kugelmann/Römer, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 56 Rn. 24 ff.

61 Ehmann, in: Gola/Heckmann (Hrsg.), BDSG, 13. Auflage 2019, § 42 Rn. 3.

62 Kugelmann/Buchmann, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 58 Rn. 82.

zu erlassen, sind eine Reihe von Maßnahmen erst deutlich nach dem 25. Mai 2018 in Gang gekommen und erlassen worden. Die betrifft insbesondere auch die Geldbußen.

Von dem Instrument der Geldbußen nach Art. 83 DS-GVO wurde durchaus Gebrauch gemacht. Allerdings ist zu beachten, dass die Mehrzahl der Fälle kleinere Verstöße betraf. Hier ging es etwa um die rechtswidrige Nutzung von Dashcams oder anderen Videoübertragungseinrichtungen oder um kleinere Fälle von Datenübermittlungen an einen falschen Adressaten. Größere Geldbußen sind in Deutschland erst wenige verhängt worden, die Zahl nimmt aber beständig zu. Diese betreffen insbesondere Unternehmen, die aus dem Bereich der Datenverarbeitung oder sozialen Netzwerke kommen und Unternehmen oder Einrichtungen aus dem Bereich der Gesundheit.

Im Fall der Geldbußen ist zudem hervorzuheben, dass aufgrund des Ordnungswidrigkeitengesetzes die ordentliche Gerichtsbarkeit zuständig ist. Klagen gegen Geldbußen gehen vor das Amtsgericht, also den Einzelrichter, und haben dort oftmals insoweit teils Erfolg, als die Geldbuße verringert wird. Die Regelung des § 41 BDSG, die das Ordnungswidrigkeitengesetz für das Datenschutzrecht in Bezug nimmt, legt eine Neuerung fest, da im Fall einer festgesetzten Geldbuße, die den Betrag von 100.000 Euro übersteigt, das Landgericht entscheidet (§ 41 Abs. 1 Satz 3 BDSG).[63] Bisher ist allerdings keine Entscheidung eines Landgerichts in diesem Zusammenhang ersichtlich.

Die Priorisierung erfolgt anhand von Schutzgütern und anhand des Risikos für diese Schutzgüter, weil dies dem risiko-basierten Ansatz der DS-GVO entspricht. Ein einschlägiges Kurzpapier der Datenschutzkonferenz (DSK) zur Risikobewertung geht in diese Richtung.[64] Die Kontrollorientierung erfolgt gegenüber den Wirtschaftsteilnehmern, die an der Verarbeitung von Daten selbst verdienen und ihr Geschäftsmodell entsprechend auf Datenverarbeitung ausgerichtet haben. Online-Banken, soziale Netzwerke zur Erleichterung von Kommunikation in bestimmten wirtschaftlichen Zusammenhängen oder Unternehmen, die Apps betreuen und organisieren, stehen eher im Fokus der deutschen Datenschutzaufsichtsbehörden als kleinere und mittlere Unternehmen des Einzelhandels oder der verarbeitenden Industrie.

Eine besondere Gewichtung gibt Art. 9 DS-GVO vor. Die dort festgelegten besonderen Kategorien personenbezogener Daten erfordern besondere Maßnahmen vom Verantwortlichen und stehen damit auch unter besonderer Beobachtung durch die Datenschutzaufsichtsbehörden. Dies betrifft insbesondere Gesundheitsdaten. Gesundheit ist ein wesentlicher infrastruktureller Aspekt des gesellschaftlichen Lebens. Von der Digitalisierung im Gesundheitswesen sind nicht nur viele Bürgerinnen und Bürger betroffen, zugleich geht es um besonders sensible Daten, die Aussagen über privateste und

63 Brodowski/Nowak, in: Wolff/Brink (Hrsg.), Beck-OK (28. Edition), § 41 BDSG Rn. 36.

64 Kurzpapier Nr. 18 (https://datenschutzkonferenz-online.de/kurzpapiere.html).

intimste Dinge beinhalten. Deren Verarbeitung bedarf besonderer Aufmerksamkeit.[65] Vor diesem Hintergrund sind Krankenhäuser oder Einrichtungen, die entsprechende Abrechnungen von Arztbesuchen vornehmen, besonders intensiv zu beobachten. Zugleich sind hier auch Beschwerden zu verzeichnen, die von Patientinnen und Patienten vorgebracht werden.

Eine Möglichkeit, Spielräume zu nutzen, bietet die Beratung. Die Beratung privater und öffentlicher Stellen wird traditionell als Aufgabe von den Beauftragten wahrgenommen. Jedoch enthält die DS-GVO keine umfassende Aufgabe der Beratung. Die Maßnahmen, mit denen Veranstaltungen durchgeführt, Informationsmittel veröffentlicht oder Verantwortliche mit Empfehlungen für die Ausgestaltung der Datenverarbeitung unterstützt werden, werden auf Art. 57 Abs. 1 lit. b DS-GVO gestützt. Die Setzung von Prioritäten obliegt dem jeweiligen Beauftragten. Das Verhältnis von Beratung zu eingreifenden Maßnahmen oder Sanktionen kann daher in den Ländern unterschiedlich gestaltet sein.

Die DS-GVO hat die Arbeitsweise der Behörden in der Bundesrepublik Deutschland verändert. Vor dem Wirksamwerden der Datenschutz-Grundverordnung waren auch vielfach informelle Möglichkeiten gegeben. Nunmehr ist die Tätigkeit der Datenschutzaufsichtsbehörden sehr viel stärker behördlich geprägt, weil sie Eingriffsverwaltung betreiben. Eine Reihe von Maßnahmen aus Art. 58 DS-GVO wie z.B. die Verwarnung oder Anordnung sind nach bundesdeutschem Verwaltungsrecht Verwaltungsakte. Ein Verwaltungsakt als konkret individuelle Entscheidung, um Rechte und Pflichten eines Betroffenen festzulegen, wird nach den Regeln des Verwaltungsverfahrensgesetzes erlassen. Damit sind die allgemeinen Regeln anwendbar. In der Konsequenz sind rechtsstaatlich gebotene Verfahrenshandlungen wie Anhörung oder Begründung entsprechend vorzunehmen (§§ 28, 39 VwVfG). Damit dauern die Verfahren länger, als sie teils vorher gedauert haben. Die Erweiterung der Befugnisse der Datenschutzaufsichtsbehörden durch die DS-GVO hat also zu einer stärkeren behördlichen Prägung des konkreten Tätigwerdens geführt.

Frage 12

Nach der Rechtsordnung der Bundesrepublik Deutschland können immaterielle Schäden nach § 253 Abs. 1 BGB ersetzt werden. Landläufig wird oft von „Schmerzensgeld" gesprochen. Damit sollen die Einbußen am Wohlbefinden ausgeglichen und eine Genugtuung für erlebtes Unrecht ausgesprochen werden, um zugleich künftige Verletzungen durch Abschreckung zu verhindern.[66] Fälle sind etwa die Verletzung des

65 Buchner, Datenschutz im Gesundheitswesen, 2019; Paschke, in: Specht/Mantz (Hrsg.), Handbuch des deutschen und europäischen Datenschutzrechts, 2019, § 13.

66 BGH NJW 1976, 1147.

allgemeinen Persönlichkeitsrechts, z.B. durch unautorisierte Bildveröffentlichungen, aber insbesondere auch Schmerzen nach Schadensereignissen. Die Beeinträchtigung etwa des allgemeinen Persönlichkeitsrechts muss schwerwiegenden Charakter haben. Dies ist dann der Fall, wenn den Schädiger schwere Schuld trifft oder das Persönlichkeitsrecht in erheblichem Grade verletzt wird.[67] Dabei sind die gesamten Umstände des Einzelfalles zu würdigen.[68]

Im Fall des allgemeinen Persönlichkeitsrechts ist die Rechtsgrundlage § 823 BGB, der in Abs. 1 Schadensersatzansprüche bei Verletzungen sonstiger Rechte beinhaltet. Die sonstigen Rechte bestehen hier im Grundrecht gewährleisteten Recht der allgemeinen Persönlichkeit nach Art. 1 und 2 Abs. 1 Grundgesetz.[69] Dies hat das Bundesverfassungsgericht bestätigt.[70]

Angesichts der Nähe des Rechts auf informationelle Selbstbestimmung zum allgemeinen Persönlichkeitsrecht, die beide in Art. 2 Abs. 1 Grundgesetz wurzeln, können gewisse Grundzüge der zivilgerichtlichen Rechtsprechung zu § 253 BGB auf ihre Übertragbarkeit geprüft werden. In der Einzelfallbeurteilung sind die von der Rechtsprechung zur Höhe von Bußgeldern entwickelten Ermessenskriterien zu beachten, die im jeweiligen Fall auf ihre Anwendbarkeit und ihre Reichweite geprüft werden. Dabei kann die Anzahl der betroffenen Personen, die Dauer der vorgenommenen Verarbeitung oder die Bedeutung des Grundrechtseingriffes eine Rolle spielen. Hier ist durchaus eine schutzgutorientierte Betrachtung auch für Art. 82 DS-GVO angebracht. Die Beeinträchtigung muss dabei ein gewisses Gewicht erreichen.

Jedoch dürften bei Art. 82 DS-GVO höhere Schadensersatzsummen als im Fall von Verletzungen des Persönlichkeitsrechts angemessen sein. Denn der Schadensersatz soll abschreckenden Charakter haben und Art. 82 DS-GVO erfasst nicht nur schwer wiegende Verletzungen des Datenschutzrechts, sondern jede Verletzung.[71]

Einschlägige Rechtsprechung ist bisher nur vereinzelt ersichtlich. Eine Wahrnehmung und Konsolidierung von Kriterien zur Anwendung des Art. 82 DS-GVO wird erst in einem mittelfristigen Zeitraum zu erwarten sein.

Frage 13

In der Bundesrepublik Deutschland hat kollektiver Rechtschutz keine Tradition. Der Individualrechtsschutz dominiert nach wie vor. Erst im Zusammenhang mit dem

67 BGHZ 35, 363.
68 BGH NJW 2005, 58, 59.
69 BGH NJW 2014, 2871, 2872.
70 BVerfG 34, 269; NJW 2004, 591.
71 Bergt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 Rn. 18.

Umweltschutz sind kollektive Rechtschutzmöglichkeiten eingeräumt worden. Dabei war das Europarecht in der Rechtsprechung des EuGH der Auslöser und die treibende Kraft.[72] Die Berechtigung zur Klageerhebung ist oft auf besonders anerkannte oder qualifizierte Einrichtungen beschränkt. Dies wird etwa deutlich im Fall der anerkannten Umweltverbände nach § 29 Abs. 2 BNatSchG oder im Fall von § 85 SGB IX der Verbände, die nach ihrer Satzung Behinderte vertreten. Inzwischen ist festzustellen, dass die Verbandsklage und andere Möglichkeiten kollektiven Rechtschutzes anerkannt sind.[73]

Der Art. 80 Abs. 1 DS-GVO manifestiert gewisse Anforderungen an die Organisationen der Vereinigung. Nach Art. 80 Abs. 1 DS-GVO kann eine betroffene Person eine Einrichtung, die entsprechende Voraussetzungen erfüllt, damit beauftragen, in ihrem Namen eine Beschwerde einzureichen. Dies ist eine Möglichkeit, die bisher kaum in Anspruch genommen wurde.

Das Verbandsklagerecht des Art. 80 Abs. 2 DS-GVO verwirklicht das Bundesdatenschutzgesetz nicht. Aufgrund der innerstaatlichen Gesetzgebungszuständigkeiten für die Gerichtsbarkeit kann nur der Bund eine entsprechende Regelung erlassen. Dies hat er nicht getan.

Ein datenschutzrechtliches Verbandsklagerecht bleibt damit auf das am 24.02.2016 in Kraft getretene Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechtes beschränkt.[74] Danach können Verbände und Kammern die Einhaltung datenschutzrechtlicher Vorschriften mit zivilrechtlichen Mitteln durchsetzen.[75] Nach dem neuen § 2 Abs. 2 Satz 1 Nr. 11 des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen wurde dies ermöglicht. Nach dieser Vorschrift sind auch Vorschriften, die die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten eines Verbrauchers durch einen Unternehmer betreffen, Verbraucherschutzgesetze im Sinne dieses Gesetzes. Dieses kollektive Klagerecht der Verbraucherzentralen ist damit auf das Verbraucherschutzrecht beschränkt. Weitergehende Optionen nach Art. 80 Abs. 2 DS-GVO, die darüber hinausgehende Aspekte aufgreifen könnten, wurden nicht ergriffen.[76] Der § 2 Abs. 2 Satz 1 Nr. 11 UKLRG ist nicht als Ausformung des Art. 80 DS-GVO zu verstehen.[77]

Die im föderalen Staat dezentral organisierten Verbraucherzentralen nehmen ihr kollektives Recht auf Klage aktiv wahr. Der Verbraucherzentrale Bundesverband und eine

72 Seibert, NVwZ 2013, 1040.
73 Wahl/Schütz, in: Schoch/Schneider/Bier (Hrsg.), Beck-OK VwGO, § 42 Abs. 2, Rn 228 ff.
74 BGBl. I 2016, S. 233.
75 EuGH, C-40/17, ECLI:EU:C:2019:629, Fashion ID GmbH & Co KG / Verbraucherzentrale NRW, Rn.57 f., K&R 2019, 562, hält dies unter der Geltung der Richtlinie für die zulässige Nutzung von Spielräumen.
76 Korreng, in: Gierschmann u.a., DS-GVO, 1. Aufl. 2018, Art. 80 Rn. 40.
77 Keppeler, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DS-GVO/BDSG, 1. Auflage 2018, Art. 81 Rn. 20.

Reihe von Verbraucherzentralen in etwa 8 der 16 Länder der Bundesrepublik Deutschland gehen mit Klagen auch auf dem Gebiet des Datenschutzes gegen private Unternehmen vor. Klagegegner sind dabei durchaus auch Facebook oder Google.

Nicht-Regierungsorganisationen spielen durchaus eine Rolle bei der Wahrung von Datenschutzrechten in der Öffentlichkeit. Hier geht es insbesondere um Sensibilisierung und Aufdecken von Missständen. Angesichts der schon vor der DS-GVO wichtigen Rolle der Datenschutzaufsichtsbehörden war allerdings die Durchsetzung im staatlichen Bereich verortet. Nicht-Regierungsorganisationen haben jedoch vielfach Verfassungsbeschwerden gegen staatliche Sicherheitsgesetze erhoben, die den Grundrechten auf Privatheit, informationelle Selbstbestimmung oder anderen Grundrechten widersprochen haben. Die Verfassungsbeschwerden gegen die Vorratsdatenspeicherung sind nur ein Beispiel von vielen. Zwar bedurfte es aufgrund des innerstaatlichen deutschen Prozessrechtes immer individueller Personen, die letztlich die Klagen erhoben haben. Sie wurden und werden aber unterstützt von Nicht-Regierungsorganisationen.

Frage 14

Datenschutz ist mit Datensicherheit eng verwoben. Die technischen und organisatorischen Maßnahmen nach Art. 24, 32 DS-GVO stehen in der Bundesrepublik Deutschland in enger Verbindung mit einschlägigen Regeln des IT-Sicherheitsrechts. Das Bundesamt für Sicherheit in der Informationstechnik spielt daher durchaus eine Rolle im weiteren Kontext auch des Datenschutzes. Ein Gesetzesvorhaben, das durch eine Neufassung des IT-Sicherheitsgesetzes[78] eine Erweiterung der Handlungsoptionen und Zuständigkeiten des BSI betrifft, ist gerade in Vorbereitung.

Das Bundeskartellamt hat in einer aufsehenerregenden Entscheidung gegen Facebook auch Verstöße gegen das Datenschutzrecht geahndet.[79] Die entsprechende Geldbuße gegen Facebook wird mit Verstößen gegen das Datenschutzrecht begründet. Die Wettbewerbsbehörden können durchaus schmerzhafte und weitreichende Sanktionen verhängen. Allerdings ist zu beachten, dass das Bundeskartellamt dabei auf wettbewerbsrechtliche Verstöße begrenzt ist. Das Verhältnis von Datenschutzrecht und Wettbewerbsrecht ist dynamisch.[80] Eine entsprechende Gesetzesänderung hat allerdings das Datenschutzrecht insoweit auch in den Anwendungsbereich des Gesetzes über die

78 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) v. 17.7.2015, BGBl. I 2015, S 1324.

79 BKartA (6. Beschlussabteilung), Beschluss vom 06.02.2019 - Aktenzeichen B6-22/16, BeckRS 2019, BeckRS 2019, 4895.

80 Peitz/Schweitzer, NJW 2018, 275.

Wettbewerbsbedingungen gebracht und damit dem Bundeskartellamt erlaubt, einschlägige Maßnahmen zu ergreifen.

Der Verbraucherschutz in der Bundesrepublik Deutschland ist nicht einer Behörde im Schwerpunkt zugewiesen. Vielmehr sind die Verbraucherzentralen als zivilrechtliche Vereine organisiert. Sie verfügen über besondere Befugnisse, wie etwa das Verbandsklagerecht. Der Verbraucherzentrale Bundesverband betreibt politische Einflussnahme und entsprechende Öffentlichkeitsarbeit. Dabei spielt das Datenschutzrecht durchaus eine Rolle.[81] Dies gilt auch für die Beratungspraxis der Verbraucherzentralen gegenüber Verbraucherinnen und Verbraucher.

Die Frage, ob weitere Behörden erforderlich sind, um Regulierungen im Internet oder für Systeme künstlicher Intelligenz zu schaffen, wird durchaus diskutiert. Hier ist aber tendenziell eine gewisse Zurückhaltung festzustellen. Zum einen liegt dies daran, dass mit dem Bundeskartellamt, dem BSI und den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bereits starke und mit entsprechend weitreichenden Befugnissen ausgestattete Behörden bestehen. Darüber hinaus wird der Selbstkontrolle in mehreren Zusammenhängen großer Raum gegeben. Dies betrifft etwa die Selbstkontrolle der Medien, aber auch die von Intermediären.[82] Die Verantwortlichen wie Facebook oder Google sollen selbst dafür sorgen, dass etwa strafbare Inhalte zügig gelöscht werden. Dies hat nur teilweise Erfolg gehabt. Aus diesem Grund wurde das umstrittene Netzwerkdurchsetzungsgesetz erlassen, mit dem Verantwortliche verpflichtet werden, strafbare Inhalte zu löschen.[83] Konkret betrifft dies insbesondere YouTube.

Eine Zusammenarbeit der Datenschutzaufsichtsbehörden mit anderen Regulierungsbehörden erfolgt im Einzelfall, eine entsprechende Struktur der Zusammenarbeit besteht nicht.

D Datenverarbeitung für nationale Sicherheitsbelange

Frage 15

Sicherheit gegenüber anderen Staaten betrifft insbesondere die territoriale Integrität. Neben diese äußere Sicherheit tritt die innere Sicherheit als Aufrechterhalten von Recht und Ordnung innerhalb des Staatsgebietes.[84] Diese Begriffsverwendung trägt rechtspolitischen Charakter. In der geschriebenen Rechtsordnung ist die öffentliche Sicherheit das zentrale

81 Specht, in: Specht/Mantz (Hrsg.), Handbuch des deutschen und europäischen Datenschutzrechts, 2019, § 9.

82 Paal, MMR 2018, 567.

83 Eifert, NJW 2017, 1450; Lang, AöR 143 (2018), 220; Löber/Roßnagel, ZD 2019, 71.

84 Götz, in: Isensee/Kirchhof, Handbuch des Staatsrechts III, 2. Aufl. 1996, § 79.

Schutzgut des Polizei- und Ordnungsrechts, das die Unverletzlichkeit der Rechtsordnung insgesamt bezeichnet und in der Rechtsprechung umfangreich ausgearbeitet ist.[85] In der Rechtsordnung der Bundesrepublik Deutschland wird zur Beschreibung eines Interesses an der Wahrung innerer Sicherheit auch der Begriff der „Sicherheit des Bundes oder eines Landes" genutzt. In Art. 73 Abs. 1 Nr. 10 lit. b GG wird die Gesetzgebungskompetenz des Bundes für den Verfassungsschutz festgelegt und Verfassungsschutz dabei als Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes definiert. Die Verwendung dieses Begriffs erfolgt zur Umschreibung schutzwürdiger Belange, die ein Vorgehen staatlicher Sicherheitsbehörden erlauben.

Nach § 22 Abs. 1 Nr. 2 lit. b BDSG ist die Verarbeitung besonderer Kategorien personenbezogener Daten durch öffentliche Stellen auch dann zulässig, wenn sie zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist. Derartige Regelungen sind häufig anzutreffen. Die Wahrnehmung der Aufgabe, öffentliche Sicherheit zu gewährleisten, erlaubt die Erhebung und Übermittlung von Daten. Die auf Art. 6 Abs. 1 Buchstabe c und e DS-GVO beruhenden innerstaatlichen Gesetze, die die Aufgabenwahrnehmung öffentlicher Stellen betreffen, enthalten regelmäßig derartige Vorschriften.

In der Umsetzung der Richtlinie über Polizei und Justiz 2016/680 ist im Bundesdatenschutzgesetz sowie den Landesdatenschutzgesetzen eine Abgrenzung enthalten, die auf die nationale bzw. innere Sicherheit zielt. So will § 45 BDSG die Anwendbarkeit der umsetzenden Vorschriften auf die Nachrichtendienste ausschließen.[86] Denn nach überwiegender Auffassung ist die Richtlinie nicht auf Nachrichtendienste anwendbar. In der Umsetzung der Richtlinie kann aber das innerstaatliche Recht Regelungen enthalten, die auch auf die Nachrichtendienste Anwendung finden. Denn die Nachrichtendienste sind öffentliche Stellen. Allgemeine Regelungen über öffentliche Stellungen, die keine Ausnahmetatbestände enthalten, finden daher auch Anwendung auf die Nachrichtendienste, womit das Datenschutzrecht in allgemeiner Form auf diese erweitert wird. Dies ist etwa der Fall des § 10 LDSG RP, der eine entsprechende Anwendung der Vorschriften des LDSG zur Ergänzung der DS-GVO auf Datenverarbeitungen anordnet, die nicht unter die DS-GVO fallen. Die speziellen Regelungen des Datenschutzes in den Gesetzen über den Verfassungsschutz oder den BND bleiben davon unberührt. Hier ist allerdings die Kontrollbefugnis der unabhängigen Beauftragten regelmäßig ausgeschlossen.

Fragen der Anwendbarkeit datenschutzrechtlicher Vorschriften stellen sich auch bei der Kooperation zwischen Sicherheitsbehörden. Nach § 57 BDSG haben betroffene Personen ein Auskunftsrecht. Bezieht sich die Auskunftserteilung allerdings auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den

85 Kugelmann, Polizei- und Ordnungsrecht, 2. Aufl. 2012, 5. Kap Rn 35 ff.
86 So auch § 26 LDSG RP.

Bundesnachrichtendienst, den militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stelle zulässig (§ 57 Abs. 5 BDSG). Die Vereinbarkeit dieser Vorschrift mit der Richtlinie begegnet dabei durchaus erheblichen Zweifeln.[87] Sieht der Verantwortliche von der Auskunft ab oder beschränkt er sie, kann die betroffene Person ihr Auskunftsrecht auch über den Bundesbeauftragten für den Datenschutz ausüben (§ 57 Abs. 7 BDSG). Selbst gegenüber dem Bundesbeauftragten ist aber eine Beschränkung des Auskunftsrechtes wirksam. Denn die zuständige oberste Bundesbehörde kann im Einzelfall feststellen, dass durch die Auskunft die Sicherheit des Bundes oder eines Landes gefährdet würde (§ 57 Abs. 7 Satz 3 BDSG). Damit kann etwa das Bundesamt für Verfassungsschutz als oberste Bundesbehörde die Auskunftserteilung verhindern. Auch die Vereinbarkeit dieser Regelung mit der JI-Richtlinie ist überaus zweifelhaft.

Die Vorratsdatenspeicherung in der Bundesrepublik Deutschland ist ein Thema, das seit Jahren die Rechtsprechung und den Gesetzgeber beschäftigt. Das ursprüngliche Gesetz über die Vorratsdatenspeicherung in Umsetzung der Richtlinie 2006/24/EG wurde vom Bundesverfassungsgericht für verfassungswidrig erklärt.[88] In seiner Rechtsprechung zur Vorratsdatenspeicherung hat der EuGH die Richtlinie 2006/24/EG dann in der Folge für nichtig erachtet.[89] Vor dem Hintergrund der Richtlinie 2002/58/EG zum Datenschutz in der elektronischen Kommunikation hat er zudem hohe Anforderungen an die Rechtmäßigkeit von umfassenden Eingriffen durch innerstaatliche Regelungen zur Vorratsspeicherung gestellt.[90] Eine anlasslose Vorratsdatenspeicherung dürfte kaum zulässig sein.[91]

Nach den Entscheidungen der deutschen und europäischen Rechtsprechung hat der Bundesgesetzgeber ein neues, eng umgrenztes Gesetz zur Vorratsdatenspeicherung erlassen. Auch diese gesetzlichen Regelungen zur Einführung einer Vorratsdatenspeicherung (am 10. Dezember 2015 wurde das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten beschlossen), die am 1. Juli 2017 in Kraft treten sollten,[92] begegnen jedoch Zweifeln hinsichtlich ihrer Vereinbarkeit mit dem Recht der EU. Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen in Münster hat diese

87 Kugelmann, in: Zöller/Esser (Hrsg.), Justizielle Medienarbeit im Strafverfahren, 2019, S. 205 (226 ff.).

88 BVerfG, 1 BvR 256/08, BVerfGE 125, 260 – Vorratsdatenspeicherung; dazu *Roßnagel,* NJW 2010, 1238 ff; s Scholz DVBl 2014, 197 (202).

89 EuGH (GK), Rs C-293/12 und C-594/12 – Digital Rights Ireland, Rn 44.

90 EuGH, verb Rs C-203/15 und C-698/15 – Tele2 Sverige AB und Secretary of State for the Home Department / Watson, Rn 93, 96 ff.

91 Priebe, EuZW 2017, 136; Roßnagel, NJW 2017, 696; Schiedermair/Mrozek, DÖV 2016, 89; zur Neuregelung durch den Bundesgesetzgeber Roßnagel, NJW 2016, 533.

92 BGBl. 2015 I, S. 2218; siehe den Gesetzestext unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Einfuehrung_Speicherfrist_Hoechstspeicherfrist_Verkehrsdaten.html.

Bedenken geteilt und einen einzelnen Provider von der Speicherpflicht befreit, woraufhin die Bundesnetzagentur die Umsetzung der Speicherverpflichtung zunächst generell ausgesetzt hat.[93] Die neuen Regelungen werden daher nach wie vor nicht angewendet (Stand: August 2019).

Das Bundesverfassungsgericht hat in seiner Entscheidung zur Vorratsdatenspeicherung grundlegende Aussagen zum Verhältnis des Grundrechtsschutzes auf EU-Ebene zum Grundrechtsschutz nach dem Grundgesetz getroffen, die seine generelle Linie weiterführen.[94] Dabei geht es vor dem Hintergrund der Anwendbarkeit der Grundrechte-Charta auf innerstaatliche Umsetzungsakte um die Reichweite der Durchführung gem. Art. 51 GRCh und damit um die Abgrenzung der Zuständigkeiten von BVerfG und EuGH. Das Bundesverfassungsgericht nimmt für sich in Anspruch, die Verfassungsmäßigkeit von innerstaatlichen Rechtsnormen, mit denen Unionsrecht umgesetzt wird, in vollem Umfang zu prüfen, soweit die Umsetzungs- und Handlungsspielräume des deutschen Normsetzers reichen. Infolge der unmittelbaren Anwendbarkeit von Verordnungen nach Art. 288 UAbs. 2 AEUV betrifft diese Rechtsprechung die Richtlinien. Das innerstaatliche Gesetz oder die gesetzesgleiche Regelung, die der Umsetzung dienen, ist an den innerstaatlichen Grundrechten zu messen. Der Spielraum des innerstaatlichen Gesetzgebers spiegelt sich in der Anwendbarkeit des Grundgesetzes auf die Nutzung dieses Spielraums. Im Urteil zum Europäischen Haftbefehl hat daher das Bundesverfassungsgericht das deutsche Gesetz, das den Rechtsakt der EU umsetzte,[95] für nichtig erklärt.[96]

Die Entscheidung zur Vorratsdatenspeicherung führt diese Rechtsprechung fort.[97] Das Bundesverfassungsgericht hält fest:

> *„Mit diesem Inhalt kann die Richtlinie ohne Verstoß gegen die Grundrechte des Grundgesetzes umgesetzt werden. Das Grundgesetz verbietet eine solche Speicherung nicht unter allen Umständen. Vielmehr kann sie auch unabhängig von einem etwaigen Vorrang des Gemeinschaftsrechts nach den Maßgaben der Grundrechte des Grundgesetzes zulässig angeordnet werden (s. unten IV). Eine Prüfung der angegriffenen Vorschriften insgesamt am Maßstab der deutschen*

93 OVG NRW, Beschluss vom 22.06.2017 - 13 B 238/17, in: Zeitschrift für Datenschutz (ZD) 2017, S. 485.

94 *Bäcker,* EuR 2011, 103 ff.

95 Es handelte sich um einen Rahmenbeschluss nach dem alten EUV; diese Rechtsaktform steht seit dem Vertrag von Lissabon nicht mehr zur Verfügung.

96 BVerfG, 2 BvR 2236/04, BVerfGE 113, 273 – Europäischer Haftbefehl; dazu *Tomuschat,* EuGRZ 2005, 453 ff; *Vogel,* JZ 2005, 801 ff; vgl. das Urteil des polnischen Verfassungsgerichts vom 27.4.2005, Az. P 1/05, EuR 2005, 494, in dem das polnische Umsetzungsgesetz für teilweise verfassungswidrig erklärt wurde.

97 BVerfG, 1 BvR 256/08, Rn. 186 f., BVerfGE 125, 260 – Vorratsdatenspeicherung.

> *Grundrechte gerät damit nicht in Konflikt mit der Richtlinie 2006/24/EG, so dass es auf deren Wirksamkeit und Vorrang nicht ankommt."*[98]

Die Anwendbarkeit der Grundrechte-Charta wird also nicht etwa verneint, weil es sich um ein Gesetz auf dem Gebiet des Sicherheitsrechts handelt. Die Wahrung der Sicherheit spielt allenfalls eine Rolle, um den Handlungsspielraum des die Richtlinie umsetzenden Gesetzgebers zu beschreiben. Die Grundrechte-Charta ist aber nach Auffassung des Bundesverfassungsgerichts deshalb nicht anwendbar, weil es sich nicht um die Durchführung von Unionsrecht nach Art. 51 GRCh handelt und daher die Grundrechte des Grundgesetzes zur Anwendung gelangen.[99]

Diese Rechtsprechungslinie ist in den wegweisenden Grundsatzurteilen vom 6. November 2019 zum „Recht auf Vergessen neu gezeichnet worden, insbesondere indem das Bundesverfassungsgericht entgegen seiner vorherigen Rechtsprechung für sich in Anspruch nimmt, in den vom Unionsrecht belassenen Spielräumen des nationalen Gesetzgebers selbst die Grundrechte-Charta anzuwenden.[100]

98 BVerfG, 1 BvR 256/08, Rn. 187, BVerfGE 125, 260 – Vorratsdatenspeicherung.

99 Zum Ganzen Kugelmann, in: Niedobitek (Hrsg.), Europarecht, 2. Aufl. 2019, § 4 Rn. 49 ff.

100 BVerfG Beschluss vom 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, K&R 2020, 51; Beschluss vom 6.11.2019, 1 BvR 276/17 – Recht auf Vergessen II, K&R 2020, 59.

Greece

Anna Pouliou, Virginia Tzortzi and Despina Vezakidou[*]

A Setting the Scene

Question 1

Greece adopted Law 4624/2019 to implement Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR").[1] With this Law the Greek government replaced the legislative framework regulating the establishment and operation of the Hellenic Data Protection Authority (hereinafter "HDPA"), adapted the Greek data protection legislation to the GDPR and transposed Directive 2016/680/EU ("Law Enforcement Directive", hereinafter "LED") into national law. Law 4624/2019 largely repeals Law 2472/1997 that implemented Directive 95/46/EC in Greece.[2]

Law 4624/2019 introduces a distinction between "private" and "public" bodies as controllers which, although not contrary to the provisions of the GDPR, is founded on a different perception than the one of the repealed Law 2472/1997 and its interpretation, both by courts and the HDPA.

Concerning the most notable flexibilities (opening clauses):

i. The lower age for a child's consent in relation to information society services offered directly to him/her has been set to 15 years. The processing of personal data of a child under 15 requires the consent of its legal representative;[3]
ii. The prohibition on the processing of genetic data for health and life insurance purposes is expressly provided for.[4] This prohibition should, however, be extended to the context of employment, while a provision on data that reveal a genetic predisposition would be useful;

---

* Anna Pouliou is Privacy & Data Protection Partner at Deloitte's Cyber Risk Advisory and a Member of the GDPR Multi-stakeholder Expert Group at European Commission (Business Europe Representative). Virginia Tzortzi is Assistant Professor of EU Law, Department of Law, Democritus University of Thrace and Secretary of the CIEEL Board of Directors. Despina Vezakidou is TMT and Privacy Lawyer.

1 Greek Law 4624/2019 was published in Government Gazette No A' 137/29.8.2019. Note that the law was heavily criticized by the HDPA in its Opinion No. 1/2020.

2 Art. 84 Law 4624/2019.

3 Art. 21 Law 4624/2019 - art. 8 GDPR.

4 Art. 23 Law 4624/2019 - art. 9(4) GDPR.

iii. With regard to the processing in the context of employment, the notion of employees includes employees both in the public and private sectors, jobseekers and former employees.[5] Law 4624/2019 maintains consent as a basis for legitimate processing, despite the HDPA's serious concerns about the validity of employees' consent in the context of employment. This consent could be conceived only in processing that is not directly related to the employment contract, but is intended only to provide employees with benefits, e.g. participation in a group insurance contract or in a share disposal plan. In principle, the consent should be given in writing, electronic means included. However, oral consent is not precluded. The employer must inform the employee of her right to withdraw her consent;

iv. The processing of personal data for the purposes of exercising freedom of expression, including academic freedom, is permitted when the data subject has given her explicit consent, or when the processing concerns personal data which have been publicly disclosed by the data subject, is about issues of general interest or concerns personal data of public persons and is limited to the extent necessary.[6] Under the Law 4624/2019 the freedom of the press takes precedence over the right to data protection, in the form of the non-application of the rights of the data subject, e.g. the right to erasure.[7]

In Greece, the HDPA is a constitutively appointed Administrative Authority. Article 4(c) Law 4624/2019 reiterates the definitions of article 4 GDPR and confirms the role of HDPA as a supervisory authority. The HDPA is competent to supervise the application of the GDPR, Law 4624/2019 and any regulation concerning the protection of the individual against the processing of personal data.[8]

Question 2

The Constitutional review of 2001 in Greece brought significant improvements to the strengthening and protection of fundamental rights. Particular attention should be paid to the explicit protection of personal data as provided for under article 9A of the Constitution.[9]

Article 9A, belonging to the new generation of "e-rights", focuses on electronic data processing, but also covers non-automated, conventional processing by traditional means.

5 Art. 27(2) Law 4624/2019 - art. 88 GDPR.
6 Art. 28 Law 4624/2019 - art. 85 GDPR.
7 See Opinion no. 1/2020 of the HDPA.
8 Arts 9 and 13(1)(a) Law 4624/2019.
9 *J. Iliopoulos*-Strangas, *General theory of fundamental rights* [in Greek], Athens, Sakkoulas Eds, 2018, pp. 11-12.

It is a defensive right. The protection of individuals is safeguarded towards both the State and individuals.[10] However, the right is not absolute. It is subject to restrictions, based on the principle of non-discrimination (under article 25§1 Constitution), the principle of the overriding public interest (under article 8§2 ECHR)and article 52§1 of the Charter of Fundamental Rights of the European Union (hereinafter "Charter"). Subjects of the right of article 9A are nationals as well as non-nationals in Greece. The right is granted only to individuals.

Under the Greek Constitution the right to protection of personal data of article 9A is not identical to the right to private and family life of article 9.[11] The Constitution also differentiates between article 9A and article 19, which ensures the secrecy of letters and all other forms of free correspondence or communication in any printed, verbal or electronic form. Limitation on the right is imposed by a judgment opposing its protection, for example, in cases provided for in the Penal Code, where the lift of secrecy is necessary due to necessity, proportionality or best interests.

Moreover, the Greek Constitution provides for separate, constitutionally independent administrative authorities that protect the differentiated legal rights conferred by articles 9A and 19.

The Charter should be taken into account in the interpretation of article 9A.[12] The right to data protection under article 8 of the Charter, entailing the key data protection principles associated with this fundamental right by explicitly mentioning consent, right of access and rectification, enjoys broader protection in relation to the right of article 9A of the Greek Constitution.[13] The only reference so far to article 8 of the Charter by the HDPA is in Opinion no. 4/2011 as to whether the Ministry of Finance may publicise on the internet the names of the persons with mature debts to the State on the basis of article 9 of Law 3943/2011 concerning combating tax evasion, where the HDPA took the view that such measure does not violate art. 8 Charter.[14] Under article 10(5) of Law 4624/2019, the HDPA is not competent to review personal data processing operations of the judicial and prosecutorial authorities in the context of their judicial function. However, the designation of another supervisory authority, consisting of judges, which would be responsible for the processing operations of the courts is not provided for. The resulting gap is held to be in breach of article 8(3) of the Charter.[15]

---

10 Judgment no. 1616/2012 of Symvoulio Epikrateias.

11 On the differentiated nature of the rights in article 9 and 9A see, among many, E. Papakonstantinou, *Dikaio Pliroforikis,*Athens, Sakkoulas Eds, 2010, p. 34.

12 Opinion no. 1/2009 of the HDPA, p. 5

13 *Iliopoulos*-Strangas, 2018, p. 696.

14 See Opinion no. 4/2011 of the HDPA, paras 1, 9, 1, 2.

15 See F.Panagopoulou-Koutnatzi, 'Law 4624/2019 and implementation of the GDPR: very promising, but delayed' [in Greek], *Syntagmawatch,* 9 September 2019, www.syntagmawatch.gr/trending-issues/nomos-

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Any processing of personal data should be lawful and fair according to the provisions of the GDPR.[16] In other words, lawful data processing should be fair otherwise data processing will not meet the GDPR requirements.

"Fairness" is a term with several dimensions, not only legal but also ethical and philosophical.[17] In general, as defined in the Merriam-Webster Dictionary "fair" as an adjective means something that is marked by impartiality and honesty: free from self-interest, prejudice, or favoritism.[18]

"Fairness" has not been interpreted in a specific way by Greek courts especially in the context of data protection. Thus, data controllers have interpreted and applied the principle of "fair processing" in combination with the "lawfulness" and "transparency" principle as an unseparated bunch of fundamental principles regarding data processing.

Although the Hellenic DPA refers to "fair" processing quite often in numerous Decisions and Opinions, it has not defined in a specific way the meaning of "fair" processing by setting, for example, criteria of "fairness" or providing concrete examples whereby processing is considered as "fair".[19]

Choosing the right legal basis according to article 6 GDPR is closely linked to the principle of fair processing as well as with the purpose imitation principle. The controller must not only select the appropriate legal basis prior to processing and substantiate this option in accordance with the accountability principle, but he also must inform the data subject according to articles 13(1)(c) and 14(1)(c) GDPR, as the choice of any legal base has legal effect on the exercise of the rights of the data subjects.[20]

4624-2019-kai-efarmogi-gdpr-polla-yposchomenos-alla-parallila-kathysterimenos/. All webpages referred to were visited 15 September 2019.

16 Recital 39 GDPR.

17 See for an analysis of the GDPR from an ethics perspective: V. Papakonstantinou, "What is "fair" in "fair and lawful" processing of personal data? ", http://www.papakonstantinou.me/blog-posts/what-is-fair-in-fair-and-lawful-processing-of-personal-data/.

18 See: www.merriam-webster.com/dictionary/fair.

19 See: UK ICO checklist in relation to fair processing that is used more widely by stakeholders also outside the UK including Greece. "Fairness: We have considered how the processing may affect the individuals concerned and can justify any adverse impact.-We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.-We do not deceive or mislead people when we collect their personal data", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/.

20 DPA Decision 26/2019.

In accordance with article 5(1) GDPR the personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed (purpose limitation).[21] This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Moreover, personal data should be processed only if the purpose of the processing could not be reasonably fulfilled by other means.[22]

In order to ensure that personal data are not kept longer than necessary, time limits for erasure or for a periodic review should be established by the controller.

The Hellenic DPA decided in numerous cases that for personal data to be processed lawfully and fairly, all the conditions with regard to the application of and compliance with the principles set out in article 5(1) GDPR should be met.

Furthermore, under the principle of accountability, the controller should implement all the necessary measures to comply with the principles set out in Article 5(1) GDPR and demonstrate their effectiveness.[23]

Question 4

The Greek courts have found that consent does not suffice for the processing to be legitimate, if the processing is carried out in breach of the principles that should govern the legitimate collection and processing of data.[24] Standard terms in contracts that are not negotiable are not sufficient to demonstrate that consent was given.[25]

In the employment context, the Greek courts have held that an employment contract does not obviate the lack of consent, since the processing without consent was carried out for a purpose not necessarily related to the performance of the employment contract.[26] The employer was under an obligation to seek consent of his/her employee-opposing party for the use of the latter's personal data in the trial, but he was required to inform him/her of their impending use.[27] In the same vein, it was considered that the disclosure by the employer to a third party of the amount of the compensation, received by the employee in the case of dismissal, requires a prior notification to the employee.[28]

Furthermore, the Greek courts condemn the practices followed by the banking sector. In particular, it has been decided that the processing of adverse financial data by banks

21 DPA Decision, among many, 16/2019.
22 Recital 39 GDPR.
23 DPA Decision, among many, 26/2019.
24 See art. 4(1) Law 2472/1997 and judgments nos. 2285/2001, 749/2005, 2254/2005 and 2255/2005 of the Council of State.
25 Judgment no. 147/2004 of the Athens Court of Appeal; judgment no. 5825/2019 of the Athens Court of First Instance.
26 Judgments nos 94 and 95/2003 of Symvoulio Epikrateias.
27 Judgment no. 7/2007 of the Corinth Court of First Instance.
28 Judgment no. 87/2013 of the Thessaloniki Court of Appeal.

without consent and, in particular, the transfer of personal data from a bank to a lawyer[29] or to debt collecting companies,[30] is unlawful. In addition, a fixed telephone and internet service provider was condemned as it repeatedly contacted an individual in order to promote its products, despite the explicit opposition of the individual, which had been expressed in various ways.[31] The statements contained in the insurance contracts constitute consent to the processing of health data related to the coverage of particular insurance risk.[32] The taking of photos with the consent of the depicted individual and their subsequent posting by her on the internet does not constitute consent for displaying the photos on the TV news,[33] while the data subject's consent to the processing of personal data that have been posted on Facebook, was deemed indispensable.[34]

With regard to legitimate interests as a basis for lawful processing, the Greek courts have ruled that the processing is permitted, without consent, only if it is carried out for the purpose it seeks to fulfill, and not for any other purpose, for which the consent has not been requested.[35] The legitimate interest is required to obviously override the rights of the data subject, up to the point where the fundamental freedoms are not affected.[36] Thus, the elements comprising the financial behavior of an individual, resulting in her insolvency, are amongst the personal data whose processing is allowed even without consent of the data subject, if the processing is indeed necessary to satisfy the legitimate interest of specific recipients, such as banks.[37] However, checking bank account activity, which is necessarily used for payroll of the employee-user of the system, in order disciplinary control to be exercised on her, is not legitimate, irrespective of whether it is necessary for the performance of the employment contract or to satisfy the legitimate interests of the bank.[38]

Question 5

The use of personal data in exchange for the provision of digital content or services has received attention in the Greek legal literature for three reasons: 1) because of the discussion at a global level around the risks of the use of social media following various failures of

29 Judgment no. 168/2018 of the Thessaloniki District Court.
30 Judgments nos 1319/2019 and 5825/2019 of the Athens Court of First Instance; judgments nos 437/2014 and 2887/2010 of the Athens Court of Appeal.
31 Judgment no. 629/2017 of the Heraklion Court of First Instance.
32 Judgment no. 292/2019 of the Symvoulio Epikrateias.
33 Judgment no. 5336/2015 of the Athens Court of Appeal.
34 Judgment no. 346/2015 of the Larissa Court of Appeal.
35 Judgments nos. 94/2003, 3908/2004, 2254 and 2255/2005, 3775/2012 of Symvoulio Epikrateias.
36 Judgment no.1988/2002 of the Athens Court of First Instance; judgment no. 2950/2002 of the Thessaloniki Court of First Instance; judgment no. 3833/2003 of the Athens Court of Appeal.
37 Judgment no. 2965/2017 of Symvoulio Epikrateias.
38 Judgment no. 3908/2004 of Symvoulio Epikrateias.

tech giants to ensure appropriate protection that have made it into the press in the past few years, 2) because of the discussions related to the proposed "Directive on certain aspects concerning contracts for the supply of digital content" at European level that have been taking place since 2015, and 3) because of the overall discussion about the protection of consumer rights and the proposal of the European Commission of the "New Deal for Consumers" on 11 April 2018 with proposed measures for the enforcement of the rights of consumers on the internet that the Greek civil society for consumer rights has been participating in.

The Greek privacy legal community has been following all these issues with great interest and many articles have been in the Greek press and in legal magazines[39] with opinions of Commissioner Jourova and other officials as well the late European Data Protection Supervisor Buttarelli who referred to the intersection of privacy and the proposed Directive on representative actions for the protection of the collective interests of consumers.[40]

One particular element that has received some debate by privacy professionals as well as the wider press in Greece is the use of personal data, and often times sensitive personal data, of children in particular as they are more vulnerable at the idea of obtaining digital content without realising the risks of "paying" for it with their personal data. This is particularly true as the average age of children that are exposed to the risks and benefits of the internet has already reached the age of 4 almost a decade ago according to OECD data.[41]

Therefore, while no supervisory authority decision and no jurisprudence is available yet in Greece on the issue of the conditions and the validity of the provision of personal data as counter-performance in exchange for digital content, the topic has been on public debate for a few years now. While there is awareness of the risks, there is also the understanding of the benefits of technology when safeguards are in place. "The idea that technology often forces us to cease being the owners of our data […] should lead us to the use of technology with awareness of our involvement and to the selection of those services and products that have the best protection policies of our individual rights".[42]

---

39 https://www.lawspot.gr/nomika-nea/antiprosopeytikes-agoges-kai-symvaseis-me-antallagma-prosopika-dedomena-sto-stohastro-toy.

40 https://edps.europa.eu/sites/edp/files/publication/19-01-04_opinion_new_deal_consumers_ summary_ el.pdf.

41 OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, Paris, https://doi.org/10.1787/20716826.

42 S. Tassis, 'Privacy in exchange for the development of technological innovation', *Law of Information & Communication Media*, Nomiki Vivliothiki, Vol. 2, 2014, p. 179.

Question 6

Law 4624/2019 has not made use of article 22(2)(b) GDPR and has not introduced any legislative measures in deviation of article 22(1) GDPR. This is perhaps not surprising as there has not been relevant national legislation in the pre-GDPR era in Greece and – presumably- the issue was not raised by stakeholders in the consultation process of Law 4624/2019.

Question 7

The Greek legislation on the protection of personal data does not explicitly refer to "a right to be forgotten". It was nevertheless enshrined in article 4(1)(d) and article 2 of Law 2472/1997 (which implemented Directive 95/46/EC) by providing for the erasure of the data that were not necessary for the fulfillment of a processing purpose. It was further established under article 13 of Law 2472/1997, referring to the right of the data subject to object to the processing of the data concerning her. A right to erasure is now enshrined in article 34 of the Law 4624/2019.

Google has refused the erasure of links from search results based on the applicants' names. Nevertheless, in cases where Google accepts the request to erase the links in question, the latter must be removed from both "google.gr" and "google.com" concerning access from Greece. However, this does not cover the erasure of links when the search takes place outside of Greece. Therefore, the right to erasure is only partially satisfied.[43]

The HDPA has established, as an expression of the principle of proportionality, the need to limit the retention time of adverse financial data (downgrading, availability, dismissal) as well as the limitation of the wide dissemination of adverse acts, both online and offline.[44]

The HDPA essentially confirms the approach that Article 17 GDPR relates to a right to erasure and not to a right to be forgotten. In actions brought against Google, the HDPA acknowledged a conditional erasure from the search engine results (delisting), but not from the source of the information.

Furthermore, the HDPA makes a distinction between personal data and defamatory value judgment,[45] while it renders its rulings only on the basis of specific allegations.[46] Thus, there is a tendency of self-restraint in dealing only with the violation of personal data. The practice followed by the HDPA is that if the claimant invokes in her claim an

43 Decisions nos. 83, 84, 86/2016 and 74/2018 of the HDPA.
44 Cf. Decision no. 62/2004 and Opinions no. 1/2010 and 2/2011 of the HDPA.
45 See, among many, G/S/691/3.2.2014 of the HDPA.
46 Decision no. 84/2016 of the HDPA.

offense against her personality, the DPA rejects her claim as this allegation is being examined by the competent courts.[47] In any case, the HDPA stresses that it is first necessary to submit a request to the controller before submitting a complaint to the HDPA.

The Greek courts seem to move towards the same direction. Regarding, for example, the distinction between personal data and defamation value judgments they have held that the disclosure of the score of each student on the notice boards of each school […] cannot abolish the personal character of the data, protected under Law 2472/1997.[48] Recently, the Symvoulio Epikrateias (Greek Court of State) has confirmed that when the personal data are communicated to third parties, the data subject should be previously informed in order to exercise the right of objection.[49]

Question 8

As stated in answer 1 above, the Hellenic Republic has recently enacted national legislation to implement the GDPR. Pursuant to Article 85(2) GDPR, according to which Member States are allowed to legislate to reconcile the right to data protection with the right to freedom of expression, the Greek Law 4624/2019 in its Article 28 under the title "Data processing and freedom of expression and information" sets the requirements for lawful processing:[50]

> To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including for journalistic purposes, and for academic, artistic or literary purposes, the processing of personal data shall be permitted where:
> (a) the data subject has given his explicit consent; (b) relates to personal data which has been made publicly available by the subject himself (c) outweighs the right to freedom of expression and the right to information over the subject's right to the protection of personal data, in particular on matters of general interest or when it concerns personal data of public persons; and (d) limited to the extent necessary to secure freedom of expression and the right to information, in particular when it relates to specific categories of personal data as well as criminal proceedings, convictions and related security measures; having regard to the right of the subject to private and family life.

47 Decision no.86/2010 and Proceedings 28/6/2016 of the HDPA. See also the Annual Report 2012 of the HDPA, Ch. 3.12.3.

48 Judgment no. 4796/2013 of the Thessaloniki Administrative Court of First Instance.

49 Judgment no. 1817/2018 of Symvoulio Epikrateias.

50 Recital 152 GDPR.

The following paragraph (2) allows exceptions to the right to data protection in the context of the processing of personal data for journalistic, academic, artistic or literary purposes where the following shall not apply:

> (a) Chapter II of the GDPR "Principles" except article 5; (b) Chapter III of the GDPR "Data Subjects Rights"; (c) Chapter IV of the GDPR" Data Controller and Data Processor", except articles 28, 29 and 32; (d) Chapter V of the GDPR "Transfers of Personal Data to Third Countries or International Organizations"; (e) Chapter VI of the GDPR "Independent Supervisory Authorities"; (f) Chapter VII of the GDPR "Cooperation and coherence; and (g) Chapter IX of the GDPR "Provisions relating to special cases of processing.

In general, the processing of personal data carried out solely for journalistic purposes should be compatible with the freedom of expression and information. Articles 5(1) and 9(1), read in conjunction with Article 2(1) of the Greek Constitution, establish the protection of human value, as this derives from the right to personality, as well as the right to the protection of personal data in Article 9A of the Greek Constitution.

The Constitution further stipulates the right of the press to inform the public and the corresponding claim of citizens to information, in accordance with its Article 14 (1) (freedom of expression, right to information). Pursuant to Article 5A of the Constitution, the right to be informed is necessary to enable everyone to participate in the social, economic and political life of the country.

According to the Hellenic DPA:

> The Constitution does not imply *in abstracto* the prevalence of one right over another. In other words, the scope of conflicting rights must be defined in a concrete manner, in accordance with the principles of ad hoc balancing of opposing interests and practical harmony and proportional balancing, applying the principle of proportionality which is constitutionally enshrined in Article 25 (1) in such a way that protected rights (freedom of information and citizens' right to information - Articles 14 (1) and 5A - and the right to privacy and the right to self-determination) maintain their regulatory scope. The judgment as to whether a specific processing was lawfully exercised or, on the contrary, whether it violated the right to information and the privacy affected, is so dependent on the criterion of whether that processing served the interest of the public which prevailed in the specific case of the right to privacy and to what extent the infringement was within the proportionality principle necessary for the exercise of the right to information. The principle of balancing is accepted by the Greek courts and the European Court of Human Rights

> (hereinafter "ECtHR"). According to this principle, the media have, pursuant to article 10 of the European Convention on Human Rights (hereinafter "ECHR"), and as validated by Greek Law 53/1974, the duty to inform the public of matters of public interest and respectively the public has the right to be informed of matters and cases of general interest. Especially when it comes to public life or issues of public interest, the need to inform the public is greater. For this reason, the ECtHR recognizes the role of journalists as "public watchdogs" […] Public officials cannot escape journalistic scrutiny and criticism in order to ensure that public opinion meets their public duties and the purpose of their mission.[51]

The Hellenic DPA has issued many Decisions on the conflict between the right to data protection (article 9A of the Greek Constitution) and the freedom of the press (article 14(1) and (2) of the Constitution) and the right to information (article 5A of the Constitution). In Decision 41/2017 the DPA ruled that publishing excerpts of letters concerning a judge's love life on a web site and reproducing it on web pages and in print and electronic newspapers is against data protection Law 2472/1997.[52] The Hellenic DPA also prohibited a reporter and the television station from broadcasting transcript containing illegally processed personal data.[53]

C Domestic Enforcement of Data Protection Law

Question 9

The second subparagraph of article 9A of the Greek Constitution provides that the protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law. The relevant public authority in Greece is the HDPA, a constitutionally consolidated independent Authority,[54] under the Ministry of Justice, Transparency and Human Rights.

The HDPA was established by Law 2472/1997, which transposed into the Greek law the Directive 95/46/EC. The President of the HDPA is Konstantinos Menoudakos, Honorary President of the Symvoulio Epikrateias.

51 www.dpa.gr/portal/page?_pageid=33,23093&_dad=portal&_schema=PORTAL#2.
52 See also Decisions nos. 100/2000, 24/2005, 25/2005, 26/2007, 165/2012, 16/2015, 17/2015 of the HDPA.
53 Decision no. 38/2005 of the HDPA.
54 On independence of the HDPA see judgments nos. 2279/2001 and 96/2003 of Symvoulio Epikrateias.

Law 4624/2019 defines, in detailed provisions, the function, the powers and the composition of the HDPA, while the right to bring an action for annulment of its decisions before the Symvoulio Epikrateias is also provided.

The HDPA consists of the President, the Deputy President and 6 members (and their Alternates) who are appointed for a six-year term that cannot be renewed, in contradiction to what was provided for by Law 2472/1997 (four-year term which could be renewed once). Members of the HDPA are senior state officials. The President, the Vice President or a permanent member of the Authority should be a Supreme Judge in order to avoid the risk of issuing acts that do not meet legal guarantees.

The election and appointment of the President and the members of the HDPA shall be made in accordance with Article 101A of the Greek Constitution. In particular, the members of DPA enjoy personal and functional independence.[55] Their selection is made by the Conference of the Presidents of the Parliament,[56] by a four-fifths majority of its members.[57]

The President and members of the HDPA are under a duty of confidentiality. Specific restrictions on the professional activity of members of the HDPA are introduced for a period of two years after the expiry of their term of office to ensure their independence and impartiality.[58] With a view to enhancing its flexibility, the possibility of the HDPA also acting as a unilateral body is further established.[59]

Apart from the tasks under article 57 GDPR, the HDPA may issue guidelines and recommendations and provide its Opinion on any provision, concerning the personal data protection, to be included in law.[60] The submission of a report of the HDPA's activity to the President of the Parliament and the Prime Minister is also provided for.[61]

In addition to the powers provided for under article 58 GDPR, the HDPA has access to any data and personal information, can impose sanctions and issue regulatory administrative acts to regulate specific, technical and detailed matters. Furthermore, the President of HDPA may issue a provisional order where necessary for the restriction of the processing.[62]

The HDPA has issued the first Decisions in accordance with the provisions of the GDPR. In particular, the HDPA reprimanded a controller for unlawful processing of personal data in order to send promotional messages via the Viber application.[63] Also, the

55 Art. 11 Law 4624/2019 - arts 52, 53 and 54 GDPR.
56 The composition of this body is determined by art. 13(1) of the Parliament's Rules of Procedure.
57 *Iliopoulos*-Strangas, 2018, pp. 180-181.
58 Art. 16 Law 4624/2019 - art. 54 GDPR.
59 Art. 17 Law 4624/2019.
60 Art. 13 Law 4624/2019.
61 Art. 14 Law 4624/2019 - art. 59 GDPR.
62 Art. 15 Law 4624/2019.
63 Decision no. 66/2018 of the HDPA.

HDPA reprimanded a controller for violating article 32 GDPR with regard to the security of the processing -and, by extension, Article 5(1)(f) GDPR- because the company had not updated the software and lacked adequate systems to detect security attacks or procedures for the regular assessment of safety measures.[64] The HDPA, furthermore, reprimanded banks for failing to notify a personal data breach in a timely manner.[65]

The HDPA recently imposed a fine in three cases. The first one concerned a European MEP candidate for unsolicited political communication, following a lawyer's complaint that the candidate used data from websites managed by the Bar Associations and the Plenary of the Bar Associations.[66] The second one related to the Price Waterhouse Coopers company for non-cumulative compliance with the terms concerning the application and compliance with principles under Article 5(1)(a-c) GDPR[67] and the last one the Aegean Marine Petroleum Network Inc for unlawful access and coping of all the server content, including personal data shared by both the above company and other companies in the same group as well as employees of companies outside the group.[68]

Question 10

The Hellenic DPA adopts a "selective to be effective" approach to complaints. Under article 57(1)(f) GDPR, the extent to which every complaint is examined depends on the HDPA. Before the submission of a complaint, the entitled individuals must appeal to the controller or the DPO, if appointed. Only in case the issue is not resolved, the individuals may submit a complaint to the HDPA. In case the aforementioned procedure is not followed, the HDPA might not examine the complaint. Complaints that are vague, unsubstantiated, submitted abusively, especially due to a repetitive pattern, or filed anonymously may be deemed inadmissible (archived) by the HDPA. Moreover, the order of priority in the examining of complaints is assessed by the HDPA on the basis of the importance and general interest of the subject matter in question.[69] Nevertheless, an act of the HDPA stating the unlawfulness of the processing of personal data is not legitimate, unless it is preceded by a hearing.[70]

The Constitution of Greece recognizes the HDPA as an independent administrative authority, responsible for ensuring the protection of personal data. The delegation of powers referred to in the Constitution is not subject to restrictions. Its specific case-by-case

64 Decision no. 67/2018 of the HDPA.
65 Decisions nos. 68 and 69/2018 of the HDPA.
66 Decision no. 19/2019 of the HDPA.
67 Decision no. 26/2019 of the HDPA.
68 Decision no. 44/2019 of the HDPA.
69 Art. 13(2) Law 4624/2019 - art. 57 GDPR.
70 Judgment no. 96/2003 of Symvoulio Epikrateias.

powers and the specific circumstances of monitoring may, nevertheless, be limited by law. However, the general withdrawal by law of its competence to monitor any personal data processing, which is carried out in Greece, is not constitutionally allowed.[71]

A limitation of the competences of the HDPA was set by the provisions introduced in Article 3(2) of Law 2472/1997 by article 8 of Law 3625/2007[72] and article 12(1) of Law 3783/2009. These amendments exempted from the application of Law 2472/1997 and from the monitoring by HDPA the processing carried out by judicial and prosecuting authorities. The HDPA is still not competent to monitor the processing which is carried out by courts and prosecuting authorities in the context of their jurisdictional competence.[73]

Finally, the competences of the HDPA are limited in relation to the broadcasting media, for which it shares competence with the National Council for Radio and Television (NCRTV) in the case of collecting and retaining personal data by automated means or archive. In particular, in cases concerning the same or substantially the same facts, if one of the two competent authorities has rendered a decision on the merits, the other cannot deal with the case and possibly impose sanctions.[74]

Question 11

The Hellenic DPA has frequently been issuing warnings and even "strict" warnings in the pre-GDPR era. In more severe cases, fines were being issued.

Law 4624/19 has been adopted with a delay, only a few days before the completion of this report, coming into force on 29 August 2019. Therefore, the Greek supervisory authority has been applying the GDPR sanctions directly in the meantime.

In its recent Decision 26/2019 the Hellenic DPA issued the corrective measures of article 58(2)(d) (order to bring processing operations into compliance) and a fine of EUR 150,000 pursuant to article 83 to Price Waterhouse Coopers for violations of article 5(1)(a), (b), (c) and 6(1) of Regulation 2016/679. Prior to that, minor fines were being issued by the supervisory authority, an example being Decision 13/2019 to a medical center performing unsolicited calls with -inter alia- no transparency according to article 14 GDPR regarding the identity of the caller and their contact details.

71 Opinion no. 1/2009 of the HDPA.

72 The Law 3625/2007 was issued after the Prosecutor of Areios Pagos (Supreme Civil and Criminal Court of Greece) issued Opinion 14/2007 on the use of cameras and other technical means by the police authorities at gatherings and in particular before, during or after the termination of protests.

73 Art. 10(5) Law 4624/2019. On the constitutionality of these provisions see L. Mitrou, *The General Data Protection Regulation*, Athens, Sakkoulas Eds, 2017, p. 149.

74 Decision no. 122/12 of the HDPA.

The Hellenic DPA has similarly used the reprimand of article 58(2)(b) in some cases: to the Public Power Company for violations of article 12(3) and (4) of the GDPR in its Decision 15/2019 and to a physical person for violations of article 13(3) in Decision 16/2019.

Law 4624/19 introduces additional penalties in accordance with article 84 GDPR, and in particular criminal sanctions, in its article 38:

1. Up to one year of imprisonment, if not more severely foreseen, to anyone who illegitimately a) interferes in the filing of personal data to get access to it b) copies, removes, alters, damages collects, registers, organises, corrects, stores, adapts changes, damages, recovers, searches information, relates, combines, restricts, deletes or destroys the data.
2. Imprisonment, if not more severely foreseen, for anyone who uses, disseminates, discloses by transferring, disposes, announces or renders accessible personal data that he obtained by interfering with its filing or allows persons not entitled to be informed of the data.
3. Imprisonment of at least one year and a penalty of 100,000 euro, if not more severely foreseen, if the acts under 2 above concern the special categories of personal data of article 9 (1) GDPR or data regarding the criminal convictions and offences or related security measures of article 10 GDPR.
4. Prison sentence up to ten (10) years in any of the above cases if the person responsible for these acts had the intention to create an illegal profit for himself or another person or material damage or harm to another person and the total profit or total damage incurred exceeds the amount of 120,000 euro.
5. Prison sentence and penalty of up to 300,000 euro if there was danger to the free functioning of the democracy or national security.

Finally, it is worthwhile mentioning that the Greek law, made use of article 83(7) GDPR to introduce administrative fines to be imposed on public authorities and bodies in its article 39. The Hellenic DPA can impose an administrative fine of up to 10,000,000 euro to public sector entities (as these are defined in article 39(1) of the Law) in their capacity as controllers for the following infringements:

1. Article 83 (4) (a) (except for articles 8, 27, 29, 42, 43) GDPR,
2. Article 83 (5) and (6) (except for articles 17, 20, 47, 90 and 91) GDPR
3. Article 5, 6, 7, 22, 24, 26, 27 (except for paragraph 7), 28 to 31, 32 (1) (a), 33 to 35 of the Law.

Regarding the calculation of such fine, the Law incorporates the following GDPR clauses: article 83 (2) (a), (c), (e), (g), (h), (i) and (3).

Question 12

The Greek legislation has historically awarded damages for intangible harm in several areas, such as in Civil or Criminal Law.

More specifically, the Civil Code (articles 57, 59 and 932) sets the requirements for awarding damages for intangible harm in the event of unlawful abuse of personality (personality right) and determines what a reasonable compensation is**.** According to these provisions, compensation consists either of paying a sum of money, making a corrective post in the media or whatever is required in the circumstances of each individual case.[75] Moreover, the Greek courts have held that fault or negligence are prerequisites for such compensation although this is disputed by legal scholars.

In the context of data protection, the Greek legal system regards the protection of personal data as a constitutional right deriving from the protection of personality as detailed under answer 2 above. The national Courts and the DPA respectively adopt and apply the fundamental principle of "proportionality", as laid down in article 25(1)(d) of the Greek Constitution, when determining the amount of compensation including damages for intangible harm to the data subjects. Adjusting this principle in the field of data protection, the type, the severity and the size of the penalties and fines should correspond to the gravity of the infringement in each case.

The Greek legal system on the protection of personal data explicitly referred to intangible harm. Previous Greek Law 2472/1997, article (23)(2) provided for compensation for personal data breaches and set a minimum amount of compensation for intangible harm to 5,869.40 euro. Moreover, the award for intangible harm was irrespective of any material harm. As it was ruled by the Greek Courts, this specific provision of Law 2472/1997 regarding a minimum amount of compensation is unconstitutional as it is opposed to the fundamental principle of proportionality.[76] Admittedly, after the entry into force of Regulation 2016/679, the above provision of article 23 no longer applies, since civil liability is now regulated by article 82 GDPR which does not provide for the authority of the national legislator to regulate the issue of compensation at national level.

Greek Courts have adopted the following criteria to calculate a reasonable compensation for intangible harm caused by infringements of the data protection legislation taking into account the following factors:

- The nature of the legally protected rights affected
- The extent of the infringement
- The circumstances of the data breach in each case

75 E. Alexandropoulou - Egyptiadou, Personal Data (in Greek), Nomiki Vivliothiki, 2016, pp. 187-191.

76 Thessaloniki Court of Appeal 733/2009, DIMEE 2009/614), Prof. L. Mitrou, p. 519.

– The degree of liability and
– The social and financial status of the parties

For example, the Supreme Court awarded damages of 15,000 euro for intangible harm caused by the illegal transmission of medical data (ultrasound) from a diagnostic center to an insurance company.[77]

Question 13

The Hellenic Republic has recently introduced legislative measures to facilitate representative actions in accordance with the provisions of article 80 GDPR.

More specifically, pursuant to article 41 of the new Law, under the title "Representation of data subjects", where the data subjects consider that the processing of their personal data infringes the provisions of the GDPR or Chapter C of the Law respectively, they have the right to mandate a non-profit body, organization or association to lodge a complaint and to exercise the rights referred to in articles 77 and 78 GDPR and article 20[78] of the Law on their behalf.

While there are several NGOs in Greece either active in the field of human rights and freedoms in the digital era including the right to privacy or focusing on the protection of internet users, none of them has undertaken a more specific role in data protection enforcement yet.[79]

By the time this report is filed, there are no other alternative movements in Greece such as personal data cooperatives or unions which are constituted in accordance with the Greek Law, have statutory objectives which are in the public interest and are active in the field of the protection of personal data to mitigate information or power asymmetries between data controllers and data subjects in particular in the online environment.

Greek consumer associations and civil society in general have showed interest in aspects of data protection, including the relevant risks on the internet and the "New Deal for Consumers", as mentioned under answer 5 above, that will introduce consumer class actions. That interest however has not been concretised in specific legal actions in the data protection field so far.

77 Supreme Court 2100/2009 (Areios Pagos), NoB 58 (2010), 1222.
78 Art. 20 refers to the right to an effective judicial remedy against a supervisory authority.
79 See e.g. Greek Non-Government Organization (NGO) called "Homo Digitalis" https://www.homodigitalis.gr/en/about-us.

Question 14

The HDPA cooperates with other regulators. In Greece, the independent administrative authorities for the protection of communications are, apart from the HDPA, the Hellenic Authority for Communication Security and Privacy (hereinafter "ADAE") and the Hellenic Telecommunications and Post Commission (hereinafter "EETT").

In particular, the ADAE has been established under Law 3115/2003 and according to Article 19 (2) of the Constitution. Its purpose is to ensure the confidentiality of letters and free correspondence or communication in any possible way.[80]

The HDPA and the ADAE issue a joint Act which specifies all matters related to the procedure and the implementation of the provisions of article 7 Law 3917/2011 regarding the obligations of electronic communications service providers or public communications networks with respect to the protection and security of retained data, as defined in the aforementioned law. Further, the HDPA and the ADAE issue a joint Act which provides instructions to communication service providers with regard to the notification of personal data breaches, the template of the notifications and the manner that the notifications should take place, pursuant to the provisions of article 8 of Law 4070/2012.

Apart from the constitutionally provided HDPA and ADAE, a large number of independent authorities are also provided for by law. Among them is the EETT, an independent administrative authority, having a general competence for telecommunications. The EETT supervises and regulates the telecommunications market and the market for postal services, including the internet. The relationship between the competences of the three authorities is determined by Law 3471/2006.

In addition, the HDPA cooperates on a regular basis with the Hellenic Consumers' Ombudsman. In the context of the above cooperation, the HDPA recently issued Decision 48/2018, which concerns the protection of consumers who use cards of intact transactions, concluding that the data sent by a MasterCard card via its intact operation is not only the card number and expiration date, but also other non-encrypted data about recent card movements (date of movements and the corresponding amounts). On these grounds, the HDPA has asked credit institutions, which are the issuers of problematic cards, to carry out, as processors, a series of actions.[81]

Finally, the HDPA cooperates with the National Council for Radio and Television (NCRTV), a Greek independent administrative authority that supervises and regulates the radio/television market, founded in 1989. The HDPA and the NCRTV share competence

80 Art. 1 Law 3115/2003.

81 Annual report of the HDPA, 2018, pp. 162 seq.

in the case of the collection and retaining of personal data (audio, image, text) by automated means or archive, and the *ne bis in idem* principle is applicable.[82]

D Data Processing for National Security Purposes

Question 15

The notion of "national security" is to be found in article 19 of the Greek Constitution that establishes the right to the protection of the confidentiality of any type of communication. Article 19 foresees that the law sets the guarantees under which the judicial authorities are not bound by this confidentiality for reasons of national security or for the determination of particularly serious crimes.

The procedure for the legal lifting of this confidentiality was indeed set out in detail in Law 2225/1994. Other applicable laws are 3115/2003 (establishing the ADAE analysed under question 14), 3674/2008 (strengthening the institutional framework for ensuring the confidentiality of communications), 3917/2011 (implementing Directive 2006/24), 3471/2006 (implementing Directive 2002/58) and Presidential Decree 47/2005 (on procedures and technical and organisational guarantees for the lifting of the confidentiality of communications).

> "Furthermore, the constitutional protection of the confidentiality of communications is completed with the adoption of criminal sanctions against infringers with article 370A of the Criminal Code. From these provisions it is derived that the protection of the confidentiality of correspondence and free connection and communication by any means is absolutely guaranteed not only against public bodies and companies but also against private ones".[83]

By "national security" we mean the protection of a country as a whole, its territorial integrity, and political independence from foreign powers. Despite the above mentioned robust protection framework, the term is very generic and vague and might be applied in an abusive manner.

Article 3 of Law 2225/1994 foresees the lifting of confidentiality upon request of the public authority in charge of the national security matter to the prosecutor of the Court of Appeals who will decide within 24 hours.

82 Decisions nos. 122/2012 and 140/12 of the HDPA. See also: DIMEE 4/2012, pp. 583 seq.

83 Decision 1/2017 of the Supreme Court of Greece (Areios Pagos).

Therefore, the law does not foresee any specific conditions for the lifting of confidentiality leaving room for the discretionary power of the prosecutor (not an independent authority) and not meeting the requirements for predictability and accessibility for a serious intervention on someone's privacy in accordance with the ECHR. The broad notion of national security as the basis for lifting confidentiality would be justified if the individuals under surveillance were suspected for criminal offences against national security and these matters were further defined in the law.

Furthermore Law 3917/2011 that implemented the Data Retention Directive foresees the retention of telecommunications data for a period of 12 months with the purpose of determining "particularly serious crimes". Despite the fact that the Court of Justice of the European Union (hereinafter "CJEU") has invalidated the Data Retention Directive, the implementing Greek Law is still in force.[84] The reason is that the law could not be automatically considered unconstitutional or invalid in the Greek legal order. However, the Ministry of Justice has formed a Special Legislative Committee for the proposition of annulment or amendment of the national law in order to be in compliance with the CJEU Judgment.[85]

Finally, the upcoming new ePrivacy and Data Retention Directives are anticipated in Greece as in all other EU Member States, in order to provide the appropriate guarantees for the protection of the fundamental rights of the citizens of the Union in line with the CJEU rulings and the GDPR.

84 Judgment of 8 April 2014 in Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

85 G. Tsolias, "Privacy, Data Retention And Data Protection In The Electronic Communications Sector - Providers Of Publicly Available Electronic Communications Services -Competent Supervisory Independent Administrative Authorities", *Greek Law Digest*, 5 March 2019, http://www.greeklawdigest.gr/component/k2/item/84.

Hungary

Tamás Bendik, Dániel Eszteri, Attila Kiss, Melinda Kovács, Ágnes Majsa and Katalin Siklósi-Somogyi[*]

A Setting the Scene

Question 1

1.1.

As an integral part of the legal developments aiming at and leading to democratic transition in Hungary, the fundamental right to the protection of personal data was enshrined in the Constitution of Hungary amongst other fundamental rights in 1989 for the first time.

Prior to Hungary's accession to the European Union, Act LXIII of 1992[1] regulated data processing operations at a general level and provided for a level of protection that the European Commission,[2] based on an opinion,[3] of the Article 29 Working Party, formally considered "adequate" in 2000. Upon accession Directive 95/46/EC[4] was also transposed into the Hungarian legal system by the amendment of this Act.

On 11 April 2011 a new constitution, the Fundamental Law of Hungary, was adopted, providing for a new legal basis for the regulation of data protection. Thus, Act LXIII of 1992 was repealed and its provisions were replaced by Act CXII of 2011 (hereinafter "Privacy Act") which entered into force on 1 January 2012.[5]

---

* The authors are senior experts of the Hungarian Data Protection Authority, the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság).

1 Act LXIII of 1992 of 17 November 1992 on the protection of personal data and the disclosure of information of public interest.

2 Commission Decision 2000/519/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary [2000] OJ L215/4.

3 Working Party on the protection of individuals with regard to the processing of personal data: Opinion 6/99 of 7 September 1999 (WP 24) concerning the level of personal data protection in Hungary.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

5 Act CXII of 2011 of 26 July 2011 on the right to informational self-determination and on the freedom of information. The English translation of the Act currently in force is available at: www.njt.hu/translated/doc/J2011T0112P_20190426_FIN.pdf. All webpages referred to were last visited 1 February 2020.

Both Act LXIII of 1992 and the Privacy Act created an *omnibus* data protection regime,[6] i.e. they were applicable as *leges generales* to all data processing operations regardless of the public or private legal status of those performing such operations, including also law enforcement, national security and defence sectors. Moreover, functioning as *leges speciales*, a large number of sectoral laws and rules regulated specific data processing situations.

1.2.

This sector-neutral and generally applicable nature of the Hungarian data protection regime was, to the extent possible, consciously retained by the legislator when the necessary legislative steps were taken to align the Hungarian legal system with the EU data protection reform. The Hungarian lawmaker decided not to repeal the Privacy Act but to amend it substantially in order to implement the General Data Protection Regulation (hereinafter "GDPR")[7] and to transpose the Law Enforcement Directive (hereinafter "LED") into the Hungarian legal system.[8]

Taking a number of steps,[9] this approach resulted in a legislative framework where the Privacy Act supplements a directly applicable GDPR[10] and continues to apply to all data processing operations (including law enforcement, national security and defence) under Hungarian jurisdiction.

1.3.

With regard to the issues the GDPR leaves to the national legislator to regulate, two types of provision might be distinguished: on the one hand, there are those that are indispensable in implementing the Regulation (mandatory legislation), while, on the other hand, there are the so-called *flexibility,* or *opening, clauses* providing significant leeway to introduce or maintain domestic legal requirements supplementing the rules of the GDPR.

Stemming from its general nature, the Privacy Act intends to follow to a certain extent both types of regulatory path, as detailed below.

---

6 On the features of an omnibus regime see, for instance: O. Lynskey, *The Foundations of EU Data Protection Law*, 1st ed., Oxford, Oxford University Press, 2015, pp. 15-30.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

8 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89).

9 In connection with the data protection reform, the Privacy Act was amended by Acts XIII and XXXVIII of 2018, while the sectoral laws were amended by Act XXXIV of 2019.

10 Section 2(2).

a. In order to provide an unhampered application of the GDPR, the Privacy Act *inter alia*
   - establishes the national supervisory authority, regulates its organisational structure and the procedural framework through which it exercises the tasks and powers specified in the Regulation;[11]
   - regulates the supervisory regime applicable to processing operations of courts acting in their judicial capacity;[12]
   - prescribes that data processing operations according to article 6(1)(c) and (e) of the GDPR shall be further regulated by sector-specific legislation.[13]
b. With the aim to make use of a number of opening clauses incorporated in the GDPR, the Privacy Act
   - provides for rules designed to reconcile the right to access public information with the right to the protection of personal data;[14]
   - extends, to a limited extent, the scope of data protection rules to the processing of personal data of deceased persons;[15]
   - prescribes that, with regard to data processing operations according to article 6 (1)(c) and (e) of the GDPR, a data protection impact assessment, as well as prior consultation shall be carried out during the process of drafting of the sector-specific legislation that requires processing.[16]

Further flexibilities incorporated in the GDPR, especially in Chapter IX thereof, are dealt with by sector-specific legislation.[17]

1.4.

Formerly, the Hungarian legal system provided for a single supervisory organ responsible for monitoring and promoting the enforcement of both the right to the protection of personal data and the right to freedom of information. According to Act LXIII of 1992, an ombudsman-type of institution, the *Data Protection Commissioner*, was designated to exercise this competence. The Fundamental Law of Hungary, however, shifted to an authority-type of institution, and thus the *National Authority for Data Protection and*

11 Chapters V and VI.
12 Chapter VI/A.
13 Section 5(3).
14 Chapters III and IV (relating to art. 86 GDPR).
15 Section 25 (relating to Preamble (23) GDPR).
16 Section 25/G(6) and Section 25/H(2) (relating to art. 35(10) and 36(4) GDPR).
17 See, for instance, Act XX of 1996 on national identity numbers (relating to Article 87), Chapter 5/A of Act I of 2012 on the Labour Code (relating to Article 88), Act LXVI of 1995 on the Archives (relating to art. 89).

Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság*, hereinafter "the NAIH") was established and has been operating since 1 January 2012.

Prior to the EU data protection reform these supervisory organs were empowered to monitor and enforce the application of legal requirements stemming from the fundamental right to the protection of personal data, without any exception regarding the specific characteristics of the data processing operations. Due to the EU data protection reform, this holistic approach, however had to be limited, as, according to the GDPR and the LED, the competence of the supervisory authorities shall not cover the processing of personal data "*when courts are acting in their judicial capacity*".[18] Hence, the Hungarian legislator, by the amendment of the Privacy Act, established a mechanism according to which the oversight of such data protection operations are entrusted to courts specifically empowered to carry out such supervision activity.

Question 2

With the adoption of the constitutional amendments paving the way to the democratic transition of Hungary in 1989, the Constitution had *expressis verbis* incorporated the right to the protection of personal data as a full-fledged fundamental right and thereby also clearly distinguished between the right to the protection of personal data and other fundamental rights concerning private and family life, which the Fundamental Law currently in force continues to maintain. Hence, this distinction had been an integral part of Hungary's constitutional system prior to the adoption of the Charter of Fundamental Rights of the European Union, and thus this feature of it has not had a role in the interpretation of national law regarding these fundamental rights.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The Hungarian legislator adopted and the courts have been applying the principles of purpose limitation and data minimisation following Decision 15 of 1991 (IV. 13.) of the Constitutional Court.[19] This decision declared that, in the absence of a definite purpose and for arbitrary future use, the collection and processing of personal data is

18 Art. 55(3) GDPR and art. 45(2) LED.

19 Decision 15 of 1991 (IV. 13.) of the Hungarian Constitutional Court on the use of personal data and the personal identification number hunconcourt.hu/uploads/sites/3/2017/11/en_0015_1991.pdf.

unconstitutional, and therefore personal data may only be processed for a definite and legally-justified purpose to which every stage of the process has to conform. The principle of fair processing of personal data was also provided for in Act LXIII of 1992 together with the said principles, in line with Convention ETS No. 108.

Among a number of relevant cases, a decision of the NAIH was challenged and even heard by the Curia of Hungary (Supreme Court) regarding the infringement of the said principles by a winding-up institution.[20] In 2014, the NAIH established that one of the biggest winding-up institutions had been processing a wider set of data of debtors and third parties (including the neighbours and family members of the debtors) than necessary, and thus its data processing operations concerning debt collection were unlawful. The decision, which was upheld also by the court, stated that the collection of data concerning medical condition, private and family life, and processing of tax identification numbers, as well as data on work conditions of data subjects cannot be justified by the business interests of the controller and was not necessary to exercise legal claims, and therefore violated the principles of purpose limitation and data minimisation even though data subjects have given their consent to the processing. The collection of photocopies of cards officially verifying the home address of debtors was found to be unnecessary and also infringed the principle of data minimisation, as all winding-up institutions have the statutory right to access to the national Personal Data and Address Register.

The controller appealed against the decision, and the court interpreted the principle of "fair" processing as a broader requirement for data processing than the principle of lawfulness, because, according to the court, it can be derived not only from the data subject's right to informational self-determination (protection of personal data) but also his or her right to privacy and the right to the protection of human dignity.[21] Concerning the controller's collection of third parties' data, the court also established the violation of the principle of fair processing as this activity interfered with the rights of the individuals, since it created a situation of disparity between the data controller and the data subject where the data subject was not in a position to be aware of what the data controller knew about him or her. In 2017, the Curia upheld this decision and added that no personal data may be lawfully collected if it has no effect whatsoever on the purpose for which the personal data are processed.[22]

A recent, post-GDPR decision of the NAIH reviewed the data processing of the "Sziget Festival" in relation to its check-in system.[23] The controller collected personal data during mandatory security screenings of thousands of festival guests by making copies of IDs and

20 Decision no. NAIH/2015/16/H.
21 Decision of Budapest-Capital Administrative and Labour Court No. 28.K.30.283/2016/42.
22 Decision of the Curia No. Kfv. 37.370/2017/7.
23 Decision No. NAIH/2019/55.

taking photos at the entry gate. The NAIH found that the scope of data processed (including citizenship, number and expiration date of IDs, date of birth and gender) compared to the stated purpose and the retention period of these data (one year) was excessive, violating the principles of purpose limitation and data minimisation.

Question 4

In 2016, the NAIH issued guidelines on the basic requirements of data processing in the context of employment, where it highlighted that consent is only valid when freely given and informed, adding also that data subjects are subordinated in the employment context, hence data controllers may rely on consent only in exceptional situations.

Later, a NAIH decision also regarded the consent of employees as invalid in relation to obligatory package scanning and inspection routine carried out at the entrance of a workplace.[24] The court upheld the findings of the supervisory authority that fraud and stealth prevention, as well as securing the physical integrity of employees may be regarded as legitimate interests of the employer, but such processing may not be based on consent of the data subjects.[25] The court added that it is the obligation of the employer to balance interests and take into account all the relevant factors and rights of the individuals prior to the introduction of such security measures.

A number of data subjects initiated inquiries with the NAIH aiming at the prohibition of processing operations performed on their personal data by financial providers following the withdrawal of their consent. In these cases, the decisions of NAIH and the courts[26] came to the conclusion that, based on the legitimate interests of the controller, a necessary and proportionate set of personal data may be processed lawfully (including their transfer to winding-up institutions) despite the objections of debtors.

Several court decisions interpret the validity of consent similarly to the interpretation provided by Article 29 Working Party guidelines, emphasising the criteria 'freely given and informed'.[27] Another court decision found that consent should be clear and unambiguous, therefore consent to publish voice recordings cannot be validly given by simply sharing personal information during a conversation if the data subject was not informed of such publication.[28]

24 Decision No. NAIH/2017/439/H.
25 Decision of the Budapest-Capital Regional Court No. 13.K.700.011/2018/5.
26 Decision of the Budapest-Capital Regional Court No. P. 25.023/2013/15.
27 Also ruled by Curia in Decision No. Kfv. 37.886/2015/7 and Decision No. Kfv. 37.330/2017/5.
28 Decision of the Budapest-Capital Regional Court No. P. 25.091/2016/16 and Decision No. P. 20.989/2015/13.

Question 5

5.1.

According to the information provided by the National Office for the Judiciary, the Hungarian courts have issued no final and binding decision acknowledging communication of personal data as a counter-performance in exchange for the provision of digital services, and there has been no judicial procedure in progress with the same subject either. The National Office for the Judiciary also stated that no lawsuit with a similar subject had been initiated and no legal reasoning or legal reference with a similar aspect had been expressed thus far.

5.2.

To state that there was public debate over the subject in question would be an exaggeration; nevertheless, it is worth mentioning that the draft "Guidelines 2/2019 on the processing of personal data under article 6(1)(b) GDPR in the context of the provision of online services to data subjects" (hereinafter "draft guidelines") has received strong criticism among Hungarian data protection experts. One author[29] criticised the draft guidelines, i.e. the European Data protection Board (hereinafter "EDPB"), for:

- applying the underlying conceptions of the GDPR to data processing activities that are in fact fundamentally different from those data processing activities the GDPR is meant to regulate;
- treating data protection as some kind of super law, the principles / regulations of which should be given more weight than the regulations of other areas of the law;
- intending to enforce data protection rules as some autotelic regime of norms, thereby not taking the data subjects' genuine will into consideration; finally
- applying an unduly narrow scope as regards the definition of "contract" in contradiction to the European traditions of civil law.

Unfortunately, these critical remarks were not discussed on their merits publicly.

5.3.

As for the NAIH, up to this date no decision or legal opinion has been issued in connection with the above question.

Nevertheless, the NAIH took an active part in the drafting of the abovementioned draft guidelines and managed to represent its views successfully, therefore the current version

29 Zs. Bártfai, *Opinion on the draft Guidelines 2/2019 of the European Data Protection Board*, https://gdpr.hvgorac.hu/opinion-on-the-draft-guidelines-2-2019-of-the-european-data-protection-board/.

predominantly reflects its legal point of view. (Please note that, according to the NAIH, some points still require further refinement.)

Question 6

The Hungarian legislator introduced some legislative measures that allow for certain data controllers to carry out automated decision-making (and profiling) in certain situations. Note that most of the following examples from Hungarian law had already been introduced before the applicability of the GDPR, 25 May 2018.

6.1.

Example No. 1: Act CL of 2016 on the Code of General Administrative Procedure

The Hungarian Code of General Administrative Procedure regulates general applicability of automated decision making as follows:

> *Section 40 [Automatic decision-making]*
> *Automatic decision-making shall apply if*
> a. *it is permitted by an Act or government decree,*
> b. *all data are available to the authority at the time of the submission of the application,*
> c. *decision-making does not require deliberation, and*
> d. *there is no party with opposing interests.*

Moreover, Section 42 of the same Code provides for the right to request the authority to reconsider the automatic decision in a full (human-controlled) procedure as follows:

> "*Section 42 [Adjudicating an application in a full procedure]*
> *If no appeal lies against a decision made in an automatic decision-making procedure […], the party may request the authority, within five days following the communication of the decision, to reconsider his application in a full procedure.*"

Finally, Section 80 (2) a) contains the following administrative safeguard regarding automatic-decision making:

> "*Where the authority refrains from adopting a final decision within the administrative time limit (legitimate silence), the party shall be entitled to exercise the right applied for. Legitimate silence shall be allowed if it is not excluded by*

an Act or government decree in a case which may be administered through automatic decision-making."

6.2.

Example No. 2.: Act CXXV of 1995 on national security services

The Hungarian Act on national security services regulates automated decision making in relation to the Passenger Names Record (PNR) System. In Hungary the PNR System is used to share data of air passengers between airline companies and a specialised national security agency, the Counter-terrorism Information and Criminal Analysis Centre for counter-terrorism and crime prevention purposes. The establishment of the national PNR system is based on European law.

The relevant provisions of the Act reads as follows:

Section 52/H. (6):

"The Counter Terrorism-information and Criminal Analysis Centre carries out its risk-assessment activity at first by way of automated risk assessment. If the automated risk assessment results in a hit, the Counter Terrorism-information and Criminal Analysis Centre investigates the hit individually by human intervention."

6.3.

Example no. 3.: Act LIII of 2017 on the prevention of money-laundering and terrorism financing

The Hungarian Act on the prevention of money-laundering and terrorism financing regulates automated decision making in relation to the national Financial Information Unit (hereinafter "the FIU"). The FIU's task is to analyse financial and transaction information sent by financial institutions for anti-money-laundering and anti-terrorism financing purposes. The establishment of the national FIU is based on European law.

The relevant provisions of the Act reads as follows:

Section 39. a):

"[…] The FIU during its operative analysis compares the received data with the data stored for analysis and evaluation purposes taking into account the risks specified in the national risk assessment methodology. The risks assessment is automated."

Question 7

7.1.

The NAIH has received numerous complaints/applications from data subjects regarding the right to erasure under the regimes of both Directive 95/46/EC and the GDPR. According to the NAIH's practice, it is not excluded per se that data subjects seek the authority's aid in the first place in order to exercise their right to erasure (i.e. without turning to the data controller first), nevertheless the likelihood of a breach of law shall be a precondition of any formal procedure of the authority. In other words, the NAIH encourages data subjects to turn directly to the data controller in the first place: in order to facilitate this, the authority provides detailed information for data subjects seeking counsel.

7.2.

A special aspect of the right to erasure is when it is exercised against the operators of search engines; in connection with this, we draw attention to the followings:

7.2.1.

On the basis of the information available, data subjects have oddly enough initiated judicial proceedings only in a relatively small number of cases with reference to the right to erasure. An interesting exception from this general tendency was the case where an attorney-at-law, whose father had been accused of serious criminal offences, requested the erasure of certain articles from the web page of a newspaper and the search results of the internal search engine of the webpage of the newspaper since these articles contained some indirect reference to the attorney-at-law, especially his profession. This case is also remarkable because the plaintiff (the attorney-at-law) sought judicial remedy at all possible instances of the court system, including the highest judicial forum, the Curia, which reviewed the final decision when it was challenged through an extraordinary remedy by the plaintiff.

The court of first instance rejected the plaintiff's claim, firstly, because, in the opinion of the court, the judgement of the Court of Justice of the European Union[30] (hereinafter "CJEU") was not applicable in the case contrary to the plaintiff's reasoning. The reason for this was that in the opinion of the court of first instance the said judgement had relevance only in relation to search engines, but the defendant was merely a newspaper even if it operated a search engine in relation to its website. Secondly, in the opinion of the court of first instance, the right to erasure cannot be exercised subsequently if the publishing of the personal data in question had been lawful originally, not even with respect to the passage of time. According to the court, the reason for this is that the press is also

30 Judgment of 13 May 2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Google Spain)*, ECLI:EU:C:2014:317.

responsible for providing information in relation to past events, even if they have already lost their currency.[31] On the basis of the plaintiff's appeal the Budapest-Capital Regional Court of Appeal partially overruled the judgement of the court of first instance[32], clarifying that the lawfulness of the original publication of the personal data is in fact irrelevant, in other words, the right of erasure is exercisable in case of both lawful and unlawful data processing. The court of second instance was of the opinion that the *Google Spain* judgement[33] had no relevance in the case either, the legal dispute could and should be settled purely on the basis of Hungarian legal norms (note that the plaintiff had requested erasure from the defendant in March 2016). In order to perform this, the interest to the exercise of the right of freedom of expression and information shall be balanced against the interest of the data subject's right to privacy. As a result of this balancing of interests the court of second instance found that the plaintiff's action was partially founded, a conclusion also shared by the Curia.[34]

7.2.2.

Subsequent to the publication of the guidelines on the implementation of the judgement of the CJEU in the *Google Spain* case,[35] the NAIH also published a document providing a thorough explanation of the guidelines on 28 July 2015.[36] When assessing complaints regarding the right to erasure against operators of search engines, the NAIH has consistently adhered to the aforementioned guidelines and national communication.

7.2.3.

In the NAIH's experience, the operators of search engines denying requests for erasure most often refer to the right to freedom of expression and information, further, if applicable, the data subjects' role in public life, which also invokes an enhanced need for information on the side of the public.

---

31 Decision of the *Budapest*-Capital Regional *Court* No. 27.P.22.284/2016/24.

32 Decision of the *Budapest*-Capital Regional *Court of Appeal* No. 8.Pf.20.407/2017/3.

33 Case C-131/12, *Google Spain*.

34 Decision of the Curia No. Pfv.IV.22.393/2017/4.

35 Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc. v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

36 Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), *A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a személyes adatoknak a Google keresőmotorjának találati listájából való eltávolításával kapcsolatos ügyek megítélése során figyelembe vett szempontokról*, https://www.NAIH.hu/files/2015-07-29-Tajekoztato_Google_talalati_list_eltavol.pdf (in Hungarian).

Question 8

8.1.

A significant example of a piece of legislation adopted by the Hungarian legislator pursuant to article 85 GDPR, is the Privacy Act. This Act creates a specific type of data: '*data accessible on public interest grounds*', defining it as "any data (including personal data), other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an Act for the benefit of the general public" (Section 3.6.). This implies that the legislator can specify in an Act that even personal data have to be considered public if it is justified by public interest. For example, the Act on private entrepreneurs and sole proprietorships[37] stipulates that the private entrepreneur's surname and forename, and other data specified in the Act, such as the entrepreneur's main activity, the address of its registered office and permanent establishments, shall be made available to the general public.

The Privacy Act itself also qualifies some personal data accessible on public interest grounds: Section 26 (2) declares that "the name of the person acting within the functions and powers of the organ performing public duties, as well as his functions and duties, executive mandate, his other personal data relevant to performing public duties, […] shall qualify as data accessible on public interest grounds". Based on this provision, the NAIH confirmed several times that the remuneration of a head of an organ performing public duties shall be deemed data accessible on public interest grounds, to which any person shall be allowed to have free access. It is important to note however that the Act introduces a limit to the publicity of these data by prescribing that this type of data shall be disseminated in compliance with the principle of purpose limitation.[38]

8.2.

Some other examples of legal provisions adopted by the legislator to reconcile the right to the protection of personal data with the right to freedom of expression and information are the following:[39]

8.2.1.

The Civil Code[40] stipulates that the exercise of fundamental rights ensuring a free discussion of public affairs may limit the personality rights of public figures to an extent that is necessary and proportionate and is without prejudice to human dignity. It adds that such

37 Act CXV of 2009.

38 Section 26(2) Privacy Act.

39 Based on the notification of Hungary sent to the European Commission according to the GDPR, published on the Commission's website: https://ec.europa.eu/info/sites/info/files/hu_notification_art_51.4_84.2_85.3_88.3_90.2_publish.pdf.

40 Section 2:44 of Act V of 2013.

an act shall not violate their private and family life and home. This provision constitutes an exemption from the GDPR, relating to a specific category of data subjects, namely public figures. According to these provisions, the processing of personal data of a public figure may be lawful if the processing relates to the discussion of public affairs, the limitation of the right to the protection of personal data is necessary and proportionate, and it does not harm human dignity.

8.2.2.

The Act on freedom of the press and on the basic rules relating to media content[41] declares that exercising the right to the freedom of the press shall not violate the rights of others relating to personality, including but not limited to the right to protection of personal data, under any circumstances. This provision has to be read together with the abovementioned exemption for public figures laid down in the Civil Code. The same Act creates an exemption from the principles enshrined in the GDPR by providing the right of media content providers not to reveal the identity of any person from whom they receive information relating to their activities in providing media content in court and authority proceedings, and to refuse to surrender any document, written instrument, article or data medium that may reveal the identity of the source of information.[42]

8.2.3.

The Criminal Code creates some specific rules which aim to reconcile the right to the protection of personal data with the right to freedom of expression. These include the provisions concerning the criminal offenses of misuse of personal data, defamation, production or publication of sound or video recordings of defamatory and slanderous nature.[43]

C Domestic Enforcement of Data Protection Law

Question 9

9.1.

Article VI (3) of the Fundamental Law of Hungary states that everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. Furthermore, Article VI (4) stipulates that the application of the right to

41 Section 4(3) Act CIV of 2010.
42 Section 6 Act CIV of 2010.
43 Sections 219, 226, 226/A, 226/B and 227 Act C of 2012.

the protection of personal data and to access data of public interest shall be supervised by an independent authority established by a cardinal Act.

Based on the aforementioned constitutional provision, the Privacy Act established the NAIH and regulates its operation in detail. From an organisational perspective, the NAIH is an autonomous state administration organ; it may not be instructed in its functions and shall operate independently of other organs and of undue influence. The tasks of the NAIH may only be determined by an Act of Parliament.

9.2.

The head of the NAIH is its president. The president shall be appointed by the President of the Republic, on the proposal of the Prime Minister. The president shall be selected from those Hungarian citizens who have a law degree and the right to stand as candidates in parliamentary elections, have at least ten years of experience in auditing procedures related to data protection or freedom of information, or who hold an academic degree in either of those fields. The President of the Republic shall appoint the president of the NAIH for a term of nine years. After the termination of his mandate, the president may be reappointed on one occasion. On 29 November 2011, Dr Attila PÉTERFALVI was nominated for the position of president of the NAIH for a period of nine years beginning on 1 January 2012.

The president shall appoint a vice-president for an indefinite period to assist his work. The vice-president shall meet the requirements set out for the appointment of the President, with the provision of having at least five years' experience in procedures related to data protection or freedom of information. In the event that the president is temporarily prevented from performing his duties, or if the office of the president is vacant, the powers and duties of the president shall be exercised by the vice-president. From 1 January 2012, the post of the Vice-President is held by Dr Endre Győző SZABÓ.

As of 2019 the NAIH is allocated a staff of 114. The president shall exercise the employer's rights over the public officials and employees of the NAIH.

In accordance with the Privacy Act, the NAIH shall be responsible for monitoring and promoting the enforcement of two fundamental rights: the right to the protection of personal data and the right to freedom of information (access to data of public interest and data accessible on public interest grounds). Accordingly, the NAIH is entrusted with duties in connection with the Schengen Information System (SIS), the Customs Information System (CIS), Europol, Eurodac and the Visa Information System (VIS).

9.3.

The following chart displays the number of cases with the NAIH between 25 May 2018 and 25 May 2019:

Authority procedures ex officio	Authority procedures upon application	Administrative audits	Inquiries	Data protection consultations
31	138	419	1009	1435

During the period between 25 May 2018 and 25 May 2019, the following amounts of fines were imposed by NAIH:

- Data protection fines: 113,833.00 euro;
- Fines based on data breach notification: 37,074 euro;
- Procedural fines: 2,604 euro.

Question 10

10.1.

The NAIH conducts two types of procedure in data protection cases covered by the GDPR: 'inquiries' which are less regulated from a procedural point of view and 'administrative procedures for data protection' regulated by administrative procedural rules. An inquiry might be initiated on the basis of the complaint of the data subject (or a third party different from the data subject or the data controller/processor) or *ex officio*, while an administrative procedure for data protection is started on the application of the data subject (or his or her representative) or *ex officio*. Irrespective of the exact procedural form, the NAIH is basically obliged to deal with the complaint/application received from data subjects, except for such cases when the authority is entitled, or even obliged to reject the complainant's submission.

10.2.

The legal grounds for refusing a complaint/application are determined in a detailed manner in the relevant laws for both types of the said procedure.

10.2.1.

As for the inquiry, the legal grounds for dismissal are defined in Section 53 (2)-(3) of the Privacy Act. According to the provisions of Section 53(2) of the Act, complaints *may* be dismissed if they refer to minor infringements or if they are anonymous, thus in these cases dismissal is dependent on the deliberation of the Authority. In contrast, Section 53(3) contains an exhaustive list of the cases where complaints *shall* be dismissed without any room for deliberation, e.g. if court proceedings are in progress in connection with the complaint, or if the complaint has been re-submitted and it contains no new facts or information on its merits.

10.2.2.

As for the administrative procedure for data protection at the application of the data subject, Section 36 of Act CL of 2016 on the Code of General Administrative Procedure (hereinafter "Administrative Code") provides the general requirements of applications. Moreover, Section 60(5) of the Privacy Act also defines additional requirements regarding the form and the content, if these requirements are not met, the NAIH shall advise the applicant on one occasion to remedy the deficiencies within the prescribed time limit, indicating also the legal consequences of non-compliance, except where otherwise provided for by an Act or government decree.

According to Section 46(1) of the Administrative Code, the NAIH shall reject the application when:

a. a condition specified by law for the commencement of the procedure is not met and this Act does not attach further legal consequences thereto, or
b. an application for the assertion of the same right has already been adjudicated, on the merits, by the court or the authority and the contents of the application and the relevant legal regulations have not changed.

Further, according to Section 46(2) of the Administrative Code the NAIH may reject the application if it does not comply with formal requirements.

In addition, Section 47(1) of the Administrative Code contains an exhaustive list when a procedure shall be terminated, the reason for this is an omission of the client (the requestor) in most cases.

10.2.3.

In summary: the NAIH always acts on complaints/applications meeting the formal requirements defined in the relevant laws in a detailed manner. As it can be seen from the relevant legal regulations referred to above, there is little room for deliberation by the Authority, rejection or admissibility of complaints/applications is mainly based on objective criteria. It should be noted that, in cases where the formal requirements are not met, the NAIH may launch an *ex officio* inquiry/administrative procedure for data protection if it is deemed reasonable on the basis of the facts of the case. It is also worth mentioning that the NAIH acts also on submissions received from persons/organisations that are not concerned in the data processing as data subjects or as their representatives; these submissions are dealt with in inquiry procedures.

10.3.

As for the obligations of the data protection supervisory authorities derived from article 78(2) GDPR [which is supplemented by Section 60/A(6) of the Privacy Act], the NAIH informs the complainant/data subject filing a request on the progress of the

complaint/application lodged pursuant to article 77 GDPR. Furthermore, the NAIH always provides detailed information on the outcome of the case regarding both inquiries and administrative procedures for data protection to the complainant/data subject filing an application.

Question 11

11.1.
The corrective measures provided by article 58(2) and article 83 GDPR have not invoked radical changes in the sanctioning practice of the NAIH due to the fact that the sanctions specified therein were available to the authority in the pre-GDPR-period, too. Of course, article 83(4)–(6) empowers the NAIH to impose significantly higher administrative fines, nevertheless, neither the maximum amount nor the percentage cap determined in the abovementioned articles has been reached.

11.2.
It is also worth mentioning that, on the basis of article 58(7) of the GDPR, the Hungarian legislator has introduced certain restrictions regarding the amount of the fine if the data controller is a budgetary agency:

> "The amount of the fine shall be between one hundred thousand and twenty million forints if the fine is imposed:
> […]
> b) pursuant to article 83 of the General Data Protection Regulation and the party required to pay the fine imposed in a decision adopted in accordance with an authority procedure for data protection is a budgetary organ."[44]

11.3.
As for the existence of additional sanctions adopted by the national legislator, according to Section 75/A of the Privacy Act:

> "The Authority shall exercise its powers specified in article 83(2) to (6) of the General Data Protection Regulation according to the principle of proportionality, in particular by primarily issuing, in compliance with article 58 of the General Data Protection Regulation, a warning to the controller or processor for the purpose of remedying the infringement when the provisions,

44 Point b) of Section 61(4) Privacy Act.

laid down by law or a binding legal act of the European Union, on the processing of personal data are first infringed."

Question 12

Damages for intangible harm as a result of violation of personality rights have been awarded by both the former Act IV of 1959 and Act V of 2013 on Civil Code (hereinafter "the Civil Code") currently in force. While Act IV of 1959 awarded 'non-pecuniary damages' in case of extra-contractual liability and to any person whose personality rights have been violated only in case of some kind of immaterial disadvantage was proven, the Civil Code replaced it by a conceptually new institution, the right to claim a 'grievance award' *(Schmerzensgeld, solatium doloris)* in case a non-material harm was done to him. Under Section 2:52(2) of the Civil Code, "conditions of the obligation to pay grievance award, and in particular the identification of the person who is under the obligation to pay and the ways of exculpating him, shall be governed by the rules on liability for damages, with the proviso that, apart from the fact of the violation, there is no need to prove further loss."[45]

The Civil Code stipulates that the court shall determine the amount of the grievance award in one sum, taking into account the circumstances of the case, in particular the gravity of the violation, whether it was committed on one or more occasions, the degree of fault, and the impact of the violation on the aggrieved party and his environment.[46]

Following general guidance and the case law of higher courts, judges must consider,[47] at their own discretion, all circumstances of the case.[48] The amount of the grievance award should be appropriate to compensate the harm or loss done and to prevent from further violations,[49] and calculated based on:

- the severity of the infringement;
- the repetition of the infringement;
- the degree of fault;
- the impacts of the infringement on the victims and on their environment, including changes to their mental or physical condition;
- and any other, even subjective elements, that may have effects on the given case.[50]

45 See also Á. Fuglinszky, 'Risks and Side Effects: Five Questions on the 'New' Hungarian Tort Law', *ELTE Law Journal*, Vol. 2, 2014, pp. 201-202.

46 Section 2:52(3) Civil Code.

47 Cs. Szabó, '"*A sérelem bére" – új bírói gyakorlat a nem vagyoni sérelem megítélése kapcsán.*' Polgári Jog, Vol. 2017/9.

48 Section 279 (3) Code of Civil Procedure (Act CXXX of 2016).

49 Decision of the Curia No. Pfv.IV.20.903/2016/7.

50 Opinion of the judicial college of the *Budapest*-Capital Regional *Court of Appeal* No. 1/2013 (VI. 17.).

In case of the violation of personality rights, in particular the right to keep personal secrets and the right to the protection of personal data and the right to the protection of one's image and recorded voice, the data subject may claim a grievance award from a data controller even after an inquiry of the NAIH has been concluded.

Question 13

The general provisions for representation are laid down in the Civil Code, providing that a juridical act may also be made via another person. The right of representation may be based, among other things, on an authorization (power of attorney), the rules of which are also detailed in the Civil Code.[51] Given that the general rules of representation and data protection enforcement procedures allow for a great flexibility, and therefore the enforcement of data subjects' data protection rights is not and was not burdensome before the GDPR, the legislator did not introduce additional measures to the pre-existing ones following the entry into force of the GDPR.

There are several ways in which the data subject can enforce his data protection rights, in which the possibilities for representation can be summarized as follows:

13.1.
Any person shall have the right to initiate an inquiry with the NAIH free of charge, by submitting a notification of an alleged infringement or an imminent threat of infringement, relating the processing of personal data. Authority inquiries can also be initiated anonymously. The NAIH may dismiss such anonymous notifications without examining it on its merits, however, it is the consistent practice of the Authority, that it conducts the inquiry based on such notifications, unless it is not possible to investigate the infringement. Since there are no specific rules laid down in the Privacy Act, the general rules of representation, as explained above, are applicable. Consequently, the data subject can also authorise an NGO by a power of attorney to act on his behalf before the NAIH.[52]

13.2.
If the data subject considers that the processing of personal data relating to him infringes the GDPR, he can submit an application for commencing an administrative procedure for data protection.[53] The application has to meet the substantive requirements prescribed by the Privacy Act and the rules laid down in the Administrative Code. The general rules of representation under the Administrative Code prescribe that, where a party is not required

51 Sections 6:11-6:20 Civil Code.
52 Sections 52-53 Privacy Act.
53 Section 60 Privacy Act.

by an Act to proceed in person, his statutory representative or the person authorised by him or by his statutory representative may proceed in his stead, or they can proceed jointly. The representative shall provide proof of his right to represent to be able to act on behalf of the data subject.[54] Based on these provisions, an NGO, or a lawyer, providing a valid authorization may represent the data subject in administrative procedures.

13.3.

If the data subject considers that the controller or the processor infringes, in the course of processing his personal data, the GDPR or other data protection related provisions laid down in laws, he may seek judicial remedy against the controller or the processor. Any person who otherwise does not have the capacity to be a party may be a party to the court action, and the NAIH may intervene in the action in order to facilitate the success of the data subject. These judicial procedures belong to the competence of regional courts. As a general rule laid down in the Code of Civil Procedure[55], an agent authorised by the party or by his statutory representative may act as the representative of the party. The Code of Civil Procedure, however, also makes it a general rule that legal representation shall be mandatory during the litigation procedure. Consequently, it is necessary to have a legal representative, who complies with the conditions[56] laid down in the Code of Civil Procedure (for example attorneys-at-law or law firms).

Question 14

14.1.

In certain cases, the Privacy Act itself obliges the NAIH to co-operate with other authorities. Accordingly, in the event that, in the course of its procedures, the NAIH has a well-founded suspicion of a criminal offence, an infraction or a disciplinary offence, it shall initiate proceedings before the organ entitled to conduct criminal, infraction or disciplinary proceedings. The acting organ shall inform the NAIH of its opinion with respect to commencing the proceedings within 30 days and, with respect to the outcome of the proceedings, within 30 days from the time of concluding the proceedings.

14.2.

Section 22 of Act C of 2003 on electronic communications contains special rules on cooperation between the National Media and Infocommunications Authority and the

54 Sections 13-14 Administrative Code (Act CL of 2016).
55 Sections 74-76 Code of Civil Procedure (Act CXXX of 2016).
56 Section 75 Code of Civil Procedure (Act CXXX of 2016).

NAIH, according to which they shall cooperate in matters affecting the electronic communications market and information society services in cases of personal data breach. According to these rules, the National Media and Infocommunications Authority and the NAIH shall agree in writing concerning the details of their cooperation. The agreement shall be reviewed annually and made available to the public. In the agreement the National Media and Infocommunications Authority and the NAIH shall *inter alia* define the conditions of cooperation so as to ensure that personal data protection regulations are properly enforced and exercised in accordance with the law. The National Media and Infocommunications Authority and the NAIH signed a Cooperation Agreement on 20 November 2013 with a special focus on promoting the conscious use of the Internet by children.

In order to strengthen their cooperation, the NAIH and the Hungarian Competition Authority signed a Cooperation Agreement on 17 February 2015. They agreed on regular expert and management level consultations on law enforcement and legislative issues, as well as joint participation in professional events.

In March 2015, the NAIH signed a Cooperation Agreement with the Hungarian National Bank, the central bank of Hungary, with the aim of ensuring a coordinated and more effective protection of personal data of consumers using services provided by organisations controlled by the National Bank, and to promote publicity of data of public interest.

14.3.

In addition to the formal cooperation agreements, the NAIH has regular informal cooperation with other regulators, as well as with the Commissioner for Fundamental Rights including consultations, delivery of opinions and interpretation of the legislation on data protection and freedom of information.

Furthermore, the NAIH operates a legislation monitoring system, and regularly follows drafting activity relating to its competence, and, if necessary, *ex officio* delivers opinions on draft legislation or modifications proposed to bills already on the agenda of the Parliament.

D Data Processing for National Security Purposes

Question 15

Act CXXV of 1995 on national security services defines 'national security interest' as follows:

Section 74. a): National security interest: the ensuring of the independence and defending of the legal order of Hungary, in particular:

- aa) the detection of offensive attempts against the state's independence and territorial integrity,
- ab) the detection and prevention of concealed efforts to harm or threaten the state's political, economic and defence interests,
- ac) the acquirement of foreign or foreign-related information necessary for governmental decisions,
- ad) the detection and prevention of concealed efforts to unlawfully alter or disrupt the state's legal order granting fundamental human rights, functioning of the multi-party system and representative democracy or the legitimate institutions, as well as
- ae) the detection and prevention of acts of terrorism, illegal guns and drug trafficking and illegal traffic of internationally controlled goods and technologies.

Following the *Tele 2/Watson* judgment,[57] the Hungarian legislator initiated the revision and future amendment of the relevant Act about data retention periods, in particular Act C of 2003 on electronic communications. Section 159/A of that Act prescribes a general one-year time period for electronic communication service providers to retain particular personal data of their customers for law enforcement, national security and military purposes. The retained data can be provided only to law enforcement, national security and military agencies for the aforementioned purposes and only upon their official and justified request. According to publicly available information, the revision of the Act by the legislator is still ongoing.

57 Judgment of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, ECLI:EU:C:2016:970.

Ireland

Kate Colleary and Emily Gibson[*]

A Setting the Scene

Question 1

The relevant national legal instrument is the Data Protection Act 2018 (hereinafter "the 2018 Act"). This covers, *inter alia*, derogations from the General Data Protection Regulation (hereinafter "GDPR")[1]; a revised structure and new powers and functions granted to the supervisory authority (the Data Protection Commission, hereinafter "DPC"); detailed processes setting out how investigations must be carried out by the DPC; and it implements the provisions of the Law Enforcement Directive (hereinafter "LED").[2]

The DPC is the supervisory authority within the meaning of and for the purposes specified in the GDPR and the LED. It is granted powers under the 2018 Act to regulate compliance with the GDPR and the provisions of the 2018 Act.

In terms of the flexibilities incorporated in the GDPR, we have set out below the most notable, as provided for in the 2018 Act.

Article 6(1)(c) and (e) and articles 2 and 3 GDPR deal with the lawfulness of processing and allow Member States to maintain or introduce more specific provisions with regard to processing necessary for compliance with a legal obligation to which the controller is subject and processing necessary for the performance of a task carried out in the public interest.

---

* Kate Colleary: Director of Pembroke Privacy and Principal, Colleary & Co. Solicitors. Emily Gibson: Barrister, Bar of Ireland. With thanks to James Byrne BL for his assistance. Thanks for comments are also due to Maureen O'Neill of MON Legal Consulting.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

Section 38 of the 2018 Act concerns processing necessary for the performance of a task carried out in the public interest and provides that processing is lawful to the extent that it is necessary and proportionate for the performance of a function under national law.

Section 38 of the 2018 Act also allows for processing that is carried out by a controller who is an air/sea carrier for the purposes of preserving the Common Travel Area (i.e. Ireland, UK, Channel Islands and the Isle of Man).

Finally, processing will be lawful insofar as it is specified in national regulations to be enacted by the Minister for Justice, Equality and Law Reform. There is a procedure provided for these regulations which involves consultation with the DPC who may make observations on issues of concern and if the Minister proposes to proceed, despite the concerns, s(he) must give a written explanation as to why. Thus there is DPC oversight of this process.

Article 23 GDPR allows Member State law to restrict the scope of the obligations and rights provided in articles 12-22 and article 34 and, to a limited extent, article 5 GDPR. These restrictions, insofar as they have been implemented in Ireland, are set out below:

Section 59 of the 2018 Act provides that the right of a data subject to object to processing is restricted in relation to certain electoral activities and in relation to certain processing activity by the Referendum Commission.

Section 60 of the 2018 Act provides for restrictions on the obligations of controllers and rights of data subjects for important objectives of general public interest. The rights and obligations are restricted to the extent that:

a. The restrictions are necessary and proportionate -
    i. To safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State
    ii. For the prevention/investigation of crime
    iii. For the administration of tax/duties owed to the State
    iv. For legal privilege
    v. To enforce civil law claims
    vi. To estimate the controller's liability on foot of a claim.
b. where the information consists of an expression of opinion about the data subject given in confidence;
c. where the information is held by the Irish supervisory authority (the DPC); the Information Commissioner or Comptroller and Auditor General for the performance of their functions.

The rights may also be restricted by Ministerial regulation where necessary for the protection of a data subject and also where such restrictions are necessary of the purpose of safeguarding important objectives of public interest e.g. public security and safety;

investigations; immigration and other objectives and other similar important objectives set out in section 60(7).

Where further regulations may be made by the Minister, under section 60 of the 2018 Act, such regulations must undergo a consultation process with the DPC. The DPC may make observations in writing on matters which are of significant concern in relation to the proposed regulations. If the Minister proposes to proceed and make the regulations notwithstanding the DPC's concern, the Minster must give a written explanation as to why. Thus, the DPC exercises a degree of oversight on any further flexibilities allowed under this section.

Section 61 of the 2018 Act provides for the restriction of data subjects' rights where necessary for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes and where the exercise of any of those rights would be likely to render impossible, or seriously impair, the achievement of those purposes.

The 2018 Act provides the following derogations in relation to articles 86-90 GDPR:

Article 86 GDPR: Processing and public access to official documents.

Section 44 of the 2018 Act allows for the disclosure of personal data contained in a record where a request for access to the record is granted by virtue of a request under the Freedom of Information Act 2014 or a request under the Access to Information on the Environment Regulations.

Article 89(2) and (3): Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Section 61 of the 2018 Act – see above.

Question 2

The right to privacy in the national legal order

The right to privacy – as distinct from a right to data protection *per se* – has been protected in Irish law through a number of mechanisms:

i. First, at common law, a right of action existed in breach of confidence where a person had disclosed confidential information;
ii. Second, a constitutional right to private life was first recognised in McGee v. Attorney General.[3] In Kennedy v. Ireland, the Irish courts accepted that State surveillance of

3 [1974] IR 284.

journalists' phones without lawful justification constituted a breach of the journalists' rights to privacy.[4]

As well as placing limits on State action, the right to privacy can also be invoked as a constitutional tort as between private citizens. In Herrity v. Associated Newspapers (Ireland) Limited, the High Court outlined the following relevant principles:[5]

> … What does emerge from the decisions to which I have referred and in particular from the decision in Cogley v. Radio Telefis Eireann[6] are the following principles: –
> i. There is a constitutional right to privacy;
> ii. The right to privacy is not an unqualified right;
> iii. The right to privacy may have to be balanced against other competing rights or interests;
> iv. The right to privacy may be derived from the nature of the information at issue – that is, matters which are entirely private to an individual and which it may be validly contended that there is no proper basis for the disclosure either to third parties or to the public generally;
> v. There may be circumstances in which an individual may not be able to maintain that the information concerned must always be kept private, having regard to the competing interests which may be involved but may make a complaint in relation to the manner in which the information was obtained;
> vi. The right to sue for damages for breach of the constitutional right to privacy is not confined to actions against the State or State bodies or institutions.

This analysis was recently cited with approval by the Court of Appeal (Peart J.) in Nolan v. Sunday Newspapers Ltd.[7]

iii Third, the right to private life under article 8 of the European Convention on Human Rights (hereinafter "ECHR") became part of Irish law pursuant to the European Convention on Human Rights Act 2003.

4 [1987] IR 587.
5 [2011] 1 IR 228.
6 [2005] IEHC 180, [2005] 4 I.R. 79.
7 [2019] IECA 141, (Unreported, Court of Appeal, 15 May 2019).

Influence of the right to data protection

The Charter right to data protection can and does influence Irish courts when addressing questions of national privacy law.

In Dwyer v. Commissioner of An Garda Síochána,[8] the plaintiff challenged the compatibility with EU law and constitutionality of the provisions of the Communications (Retention of Data) Act 2011. The 2011 Act had originally been enacted to transpose the requirements of Directive 2006/24/EC (hereinafter "Data Retention Directive")[9] which had required mass retention of telecommunications data for law enforcement purposes namely the prevention, detection, investigation or prosecution of a serious offence, the safeguarding of the security of the State, and the saving of human life. The Data Retention Directive which mandated bulk data retention had been annulled by the Court of Justice (hereinafter "CJEU") in 2014 in *Digital Rights Ireland*, finding that "general and indiscriminate" retention was incompatible with EU law.[10] Subsequently, in 2016, the CJEU had indicated in *Tele2 and Watson* that national law data retention measures for criminal justice purposes could infringe EU law.[11] Only targeted retention to fight serious crime was acceptable.

The plaintiff had been convicted of murder in circumstances where telecommunications data obtained under the 2011 Act had been used in his trial. The Court found that the 2011 Act was incompatible with EU law due to the absence of prior independent scrutiny of the scheme of retention and access and/or safeguards against abuse.

However, the court did go on to consider the constitutional question briefly before concluding that it was unnecessary. The Court noted:

> 5.20 The Court will not make a declaration concerning the alleged repugnancy of sections 3 and 6 of the 2011 Act with the Constitution. The discussion of the invalid 2006 Directive together with the referred legislation from England and Sweden that were considered in Tele2 do not require this Court to determine the constitutionality of the impugned sections. That does not mean that the in-depth analysis by the ECJ cannot influence the reasoning to be adopted if this Court could decide or was obliged to decide on the Plaintiff's

8 [2018] IEHC 685.

9 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC 89 [2006] OJ L105/54.

10 Judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Digital Rights Ireland Ltd* [2014] ECLI:EU:C:2014:238.

11 Judgment of 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson* [2016] ECLI:EU:C:2016:970.

claim of invalidity having regard to the Constitution relating to retention and access.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

How have data controllers applied these principles?

These principles have been applied in many organisations as part of "data-mapping" projects. The principle of "fair processing" has been implemented by many organisations by drafting fair processing notices (as required by articles 13 and 14) in a fair and transparent manner. However, there remains a concern that while an organisation could be compliant with the principles of the GDPR, they must also ensure that they process personal data "fairly". This is an opaque concept which will, no doubt, be further considered by the DPC, the courts and the European Data Protection Supervisor in time.

The requirement to identify a lawful basis for processing has been widely implemented by organisations carrying out GDPR readiness projects where a lawful basis for each category of data collected is identified.

In relation to the principles of purpose limitation and data minimisation, most organisations have, as part of their data mapping exercise, identified appropriate retention periods and have reassessed their data collection processes to only collect personal data that is relevant and appropriate to the identified lawful purpose for collection.

Consideration by the DPC and the national courts:

The concepts of fair processing, purpose limitation and data minimisation have been the subject of substantial consideration by the DPC. The DPC publishes case studies of its decisions on data protection complaints and investigations to provide guidance on these issues.

In its 2018 Report, the DPC published Case Study 2 of 2018 based on a complaint handled in accordance with the GDPR and the 2018 Act which related to the provision of CCTV footage concerning a data subject by the data controller (a bar) to that data subject's employer. The DPC was satisfied that this processing by the bar was necessary in pursuit of the legitimate interests of the employer. It would have been unreasonable for the bar to refuse the employer's request in circumstances where there was an allegation that a serious assault had taken place at the bar during an employee social event. Further, there was adequate signage in the bar regarding the presence of CCTV.

Similarly, the issue of the correct use of CCTV has arisen in many previous case studies published by the DPC. In Case Study 12 of 2015 which concerned a complaint handled under the previous legislative regime of the Data Protection Acts 1988 and 2003 (which transposed the 1995 Data Protection Directive), a bus operator had, while reviewing CCTV footage in the context of a customer complaint, discovered one of its drivers using a mobile phone while driving when reviewing CCTV footage in the context of a customer complaint. The driver later complained of the use of this footage against him in a disciplinary procedure. The operator was found to have contravened the principles of fairness of data processing in circumstances where it had failed to properly or fully inform staff that CCTV footage might be used in disciplinary proceedings.

In Case Study 14 of 2018, issues of lawfulness, fairness and accuracy of processing arose in connection with data subjects incorrectly being associated with media articles by a news feature of a professional networking platform. Persons were matched by name only with media articles which was found to be insufficient and gave rise to data protection concerns.

The DPC currently has a number of statutory inquiries open in relation to complaints/potential infringements concerning cross border processing by multinational organisations for which the DPC is the lead supervisory authority, where it is examining compliance with the principle of fairness in contexts such as transparency, retention and fair processing. It is anticipated that the decisions in these cases (which will be subject to the one-stop-shop decision making process under article 60 GDPR) will provide practical reference points and guidance for controllers as to NSAs' application of the concept of fairness in high volume data processing scenarios.

The concepts have not yet received substantial judicial consideration at the level of the Superior Courts. Appeals from decisions of the DPC are heard in the first instance by the Circuit Court and are frequently further appealed to the Superior Courts.

Question 4

The concept of "legitimate interests" has received some consideration by the Superior Courts.

In EMI Records (Ireland) Ltd. v. Eircom Ltd.[12], the High Court was asked whether the processing of IP address data could be necessary for the purpose of the legitimate interests pursued by the defendant. The purpose of that processing was to identify those who might be illegally downloading copyright works from the internet. The Court approached this issue by reference to the principle of proportionality and a balancing of the right of owners of copyright to have the fruits of their labour protected, versus any right which an internet

12 [2010] 4 I.R. 349.

user might have to access the internet and not to have that access terminated. The judge recognised that the protections afforded to copyright were not limited to those provided under the Copyright and Related Rights Act 2000, but that protection of copyright was also a fundamental right afforded protection by the Constitution. This being the case, it was not only legitimate for the defendant to pursue a policy which would afford protection to copyright, but the court would expect the defendant to do so.

More recently, in B.S. v. Refugee Appeals Tribunal,[13] the appellants challenged the Tribunal's provision of information to the UK authorities as *inter alia* a breach of data protection law. The Court held:

> 63. In relation to the provision of the fingerprints to the UK as part of the information request, there is no question but that this comprises a legitimate interest for the purposes of s. 2A of the Data Protection Act, 1988. As one sees from article 4 of the Dublin III Regulation itself, the authorities here are obliged upon an application for asylum being made to inform the applicant of a number of matters including at (e) "the fact that the competent authorities of Member States can exchange data on him or her for the sole purpose of implementing their obligations arising under this Regulation". By providing to the UK authorities the fingerprints lawfully taken from the appellants, ORAC was doing so in pursuit of the legitimate interest of obtaining information relevant to the task of determining the member state responsible for examining the appellants' applications. That is a legitimate interest which fulfils the conditionality specified in s. 2A of the 1988 Act for the processing of personal data.

This finding was recently upheld by the Supreme Court in B.S. v. Refugee Appeals Tribunal[14].

In cases where the DPC has examined reliance on the legal basis of legitimate interests, it has applied the rationale of CJEU in *Rīgas*, in which it considered the application of article 7(f) of the Data Protection Directive (95/46/EC)[15] and identified three conditions that must be met in order to justify the processing.[16] These were as follows: a) there must be the existence of a legitimate interest justifying the processing; b) the processing of the

13 [2017] IECA 179.

14 [2019] IESC 2.

15 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

16 Judgment of 4 May 2017 in Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme* [2017] ECLI:EU:C:2017:336.

personal data must be necessary for the realisation of the legitimate interest; and c) that interest must prevail over the rights and interests of the data subject.

In the context of ongoing statutory inquiries by the DPC concerning systemic and high volume data processing operations by multinational organisations, there are a number of cases where the DPC is examining reliance on legal basis, including consent and legitimate interests for specific processing operations. Again, the DPC's decisions in these cases will be subject to the article 60 decision making process under the GDPR.

Question 5

In mid-2018, the Irish Government, through the Department of Business, Enterprise and Innovation issued a call for views[17] on the "New Deal for Consumers" which was announced by the European Commission in April 2018.[18] While not specifically dealing with the issue of personal data as counter-performance for the provision of digital content, this package of legislative reforms proposed, amongst other things, extending consumer rights protection to so-called "free" digital services where personal data is provided instead of payment.

Separately, the DPC has a number of inquiries currently ongoing concerning cross-border processing involving the use of personal data to conduct online targeted advertising. The DPC's decisions in these cases will again be subject to the article 60 decision making process under the GDPR.

Question 6

Section 57 of the 2018 Act provides that:

> "Subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject, the right of a data subject not to be subject to a decision based solely on automated processing, including profiling, shall, in addition to the grounds identified in article 22 not apply where—
> a. the decision is authorised or required by or under an enactment, and
> b. either

17 "Call for views on Proposed EU Directive on the Better Enforcement and Modernisation of EU Consumer Protection Rules, https://dbei.gov.ie/en/Consultations/Call-for-views-Proposed-EU-Directive-Better-Enforcement-and-Modernisation-EU-Consumer-Protection-Rules.html and also https://dbei.gov.ie/en/Consultations/Consultations-files/Call-for-views-Better-Enforcement-and-Modernisation-EU-Consumer-Protection-Rules.pdf. All webpages referred to were visited on 29 February 2020.

18 Review of EU consumer law - New Deal for Consumers, www.ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en.

i. the effect of that decision is to grant a request of the data subject, or
ii. in all other cases adequate steps have been taken by the controller to safeguard the legitimate interests of the data subject which steps shall include the making of arrangements to enable them to make representations/request human intervention/request to appeal the decision."

The "suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject" are set out at section 36 of the 2018 Act and include:

a. explicit consent of the data subject for the processing of his or her personal data for one or more specified purposes,
b. limitations on access to the personal data undergoing processing within a workplace in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data,
c. strict time limits for the erasure of personal data and mechanisms to ensure that such limits are observed,
d. specific targeted training for those involved in processing operations, and
e. having regard to the state of the art, the context, nature, scope and purposes of data processing and the likelihood of risk to, and the severity of any risk to, the rights and freedoms of data subjects -
    i. logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased,
    ii. in cases in which it is not mandatory under the Data Protection Regulation, designation of a data protection officer,
    iii. where the processing involves data relating to the health of a data subject, a requirement that the processing is undertaken by a person referred to in section 52 (2),
    iv. pseudonymisation of the personal data, and
    v. encryption of the personal data.

Additional suitable and specific measures may be introduced by regulation.

In making such regulations the Minister shall have regard to the public interest and the need for protection of individuals with regard to the processing of their personal data and in particular—

a. the nature, scope, context and purposes of the processing,
b. risks arising for the rights and freedoms of individuals, and
c. the likelihood and the severity of the risks for the individuals concerned.

Question 7

Following the Judgment of 13 May 2014 in *Google Spain*[19] search engines throughout the EU introduced "Right to Be Forgotten" processes to facilitate the exercise of these rights.

In Savage v. Data Protection Commissioner,[20] Mr. Savage sought to have a Reddit discussion delisted from Google search results. He had been a candidate in the local elections in 2014 and the article criticised his campaign material, describing him as a "homophobic" candidate. Google had refused to delist the result and the DPC had found no contravention of data protection law. However, on appeal in the Circuit Court, the Judge had upheld Mr. Savage's appeal on the narrow basis that the heading of the Reddit discussion, describing Mr. Savage as homophobic, did not make it clear that that was the individual Reddit poster's opinion. It therefore risked inaccuracy.

On appeal, the High Court considered an argument that the Circuit Court had been obliged to consider the entirety of the text of the Reddit discussion rather than merely the heading and held:

a. That the Circuit Court Judge had been wrong to consider the URL heading in isolation as that Court "in applying the jurisprudence of Google Spain had a duty to consider the underlying article the subject of the search";[21] and
b. That, if the court had considered the underlying discussion thread it could not have come to the conclusion that it was inaccurate data and factually incorrect, or an appearance of fact.[22]

Notably, the Court held Google had not been obliged to edit the search results to place parenthesis around the URL heading. The responsibility placed on the data controller by the CJEU in *Google Spain* was to delist the search once appropriate criteria were considered.

During the period from 25 May to 31 December 2018 (on which the DPC's first annual report under the GDPR was based), approximately 25% of all cross-border processing complaints received by the DPC under the one-stop-shop mechanism related to exercise of the right to erasure/ right to be forgotten. In a large proportion of such cases, complaints are not dealt with by the DPC but are handled locally by the receiving National Supervisory Authority (hereinafter "NSA"). This is generally for either of two reasons. Firstly, with complaints relating to the Google search engine, the controller in question is not Google Ireland Limited but rather is Google LLC in the US (it not having a main establishment in the EU) and so the DPC is not the lead supervisory authority. Accordingly, the

19 Judgment of 13 May 2014, *Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.
20 [2018] IEHC 122.
21 Ibid, para. 35.
22 Ibid, para. 36.

one-stop-shop mechanism does not apply and rather each NSA in the EU has competence to handle such complaints under article 55 GDPR. Secondly, where right to be forgotten complaints which relate to cross border processing by other controllers are received, these will also generally be handled locally by the receiving NSA (and not the DPC even where it is the lead supervisory authority) under article 56(2) GDPR as a derogation from the principle of the lead supervisory authority's competence. This is because such cases will generally involve an assessment of a single data subject request in the context of local, on-the-ground conditions.

Question 8

Section 43(1) of the 2018 Act provides that processing of personal data for the purpose of exercising the right to freedom of expression, including *inter alia* processing for journalistic purposes, is exempt from compliance with certain provisions of the GDPR "where, having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with the provision would be incompatible with such purposes". Provision is also made for the DPC to make a referral to the High Court for its determination on any question of law relating to whether a specific processing operation is exempt on grounds of freedom of expression and information, from compliance with a provision of the GDPR.

Section 43(1) suggests a balancing approach similar to that adopted in respect of journalistic privilege in other areas of national law. The national law concept of journalistic privilege is heavily influenced by the case law of the European Court of Human Rights (hereinafter "ECtHR"). In Mahon v. Keena,[23] the Supreme Court considered the scope of journalistic privilege in the context of confidential information having been leaked from the Planning Tribunal to a national newspaper. The Court referred to the following passage from the judgment of the ECtHR in *Goodwin v. United Kingdom*:[24]

> Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable

23 [2010] 1 I.R. 336.
24 (1996) 22 E.H.R.R. 123.

> information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with article 10 of the Convention unless it is justified by an overriding requirement in the public interest.

The Supreme Court went on to refer to the test set by the Strasbourg Court: "[t]he court laid emphasis on the need for any restriction on freedom of expression to be 'convincingly established'. It said that the 'national margin of appreciation is circumscribed by the interest of democratic society in ensuring and maintaining a free press'. Therefore, 'limitations on the confidentiality of journalistic sources call for the most careful scrutiny by the court'".

C Domestic Enforcement of Data Protection Law

Question 9

The relevant public authority in Ireland is the DPC.

Composition:
No more than three members; each being known as a Commissioner for Data Protection (a Commissioner). There is currently only one Commissioner, Helen Dixon, who was recently reappointed to the role for a further term of 5 years. Where there is more than one Commissioner, a chairperson may be appointed by the Minister.

Appointment process for members and staff:
A Commissioner is appointed by the Government on the recommendation of the Public Appointments Service for a period of not less than 4 and not more than 5 years from the date of appointment. The Public Appointments Service appoints a selection panel and holds an open selection competition. It must ensure that a person is recommended for appointment only if it is satisfied that the person has the qualifications, experience and skills necessary to enable the DPC to effectively perform its functions. A Commissioner whose term expires may be reappointed for one further period of not less than 4 and not more than 5 years without the need for a further open selection process.

Staff may be appointed by the DPC and such staff are civil servants.

Additional power or duties the NSA is entrusted with under national law:
In addition to the functions assigned to the Commission as the NSA under the GDPR and the LED, there are a number of general functions included within the DPC's role including all functions assigned under the 2018 Act and other functions as may be assigned from time to time by other enactment. In addition to specific data protection legislation, there are in the region of 20 other pieces of legislation, spanning a variety of sectoral areas concerning the processing of personal data, where the DPC must perform a particular supervisory function assigned to it under that legislation.

The DPC is also the relevant supervisory authority for the purposes of processing of personal data in the context of certain electronic communications (including, amongst other things, unsolicited electronic communications made by phone, e-mail, and SMS) under the specific laws set out in the "ePrivacy Regulations" (S.I. No. 336 of 2011), under which the ePrivacy Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC)[25] was transposed into Irish law.

The DPC also monitors the lawfulness of processing of personal data in accordance with Regulation (EU) No 603/2013[26] – on the establishment of Eurodac.

The DPC is designated for the purposes of Chapter IV (Mutual assistance) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.

Details regarding its 'enforcement record' under the GDPR:
During 2019 (the first full calendar year of application of the GDPR), the DPC received in excess of 6000 valid data breach notifications, over 700 new DPO notifications (bringing the total number of such notifications to 1596 at year end) and in excess of 7000 complaints. Over 450 cross-border processing complaints were received through the GDPR's One Stop Shop mechanism. There were nearly 48,500 contacts made with the DPC's Information & Assessment unit in this period. During 2019 there were also 70 statutory inquiries underway at the DPC, examining matters of compliance under the GDPR and the LED as transposed, including 21 GDPR inquiries relating to international tech companies. In 2019,

25 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

26 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2013] OJ L180/1.

the DPC concluded its first inquiry and issued a decision under the Irish Data Protection Act 2018 (specifically under the provisions that transpose the LED) in relation to An Garda Síochána (the Irish police force).[27] This included the exercise of three corrective powers (a reprimand, an order to bring processing into compliance and a temporary ban on processing). The first decisions (and exercise of corrective powers if there are findings of infringements) arising from inquiries in relation to compliance with the GDPR (including relating to international tech companies) are expected during the first half of 2020.

Question 10

There is a formal complaint handling process set out in detail in Chapter 2 of Part 6 the 2018 Act which gives further effect to the obligation on NSAs under article 57.1(f) GDPR to handle every complaint and investigate it to the extent appropriate. (A separate but equivalent process for the handling of complaints under the LED as transposed is set out in Chapter 3 of Part 6). It provides that the DPC must examine the complaint and take such action in respect of it as the DPC considers appropriate having regard to the nature and circumstances of the complaint. The DPC may take such steps to arrange or facilitate an amicable resolution of the complaint. Where an amicable resolution cannot be reached within a reasonable time, unlike under the previous legislative regime in Ireland, the DPC is not under an obligation to reach a statutory decision in relation to each and every complaint it receives. Instead there is a range of tools available to the DPC, e.g. reject or dismiss the complaint, provide advice to the complainant; serve an enforcement notice on the controller or processor; undertake such inquiry as the DPC thinks fit and take such other action as the DPC considers appropriate. Consistent with the obligations under articles 77 and 78 GDPR, the DPC must update the complainant on the progress of his or her complaint within 3 months after it has been received and must also give the complainant a notice in writing, informing him or her of the ultimate action taken in relation to the complaint.

As set out in its first annual report on its activities under the GDPR, the DPC's fundamental objective in handling the very large volumes of complaints which it receives is to vindicate the rights of data subjects. As stated in that annual report, in the DPC's experience, a high proportion of the complaints which it handles are amenable to being amicably resolved in a timely fashion without the DPC's having to consider whether it

27 In relation to the DPC's enforcement record under the pre-GDPR regime of the Data Protection Acts 1988 and 2003, see also the DPC's report and ensuing enforcement action in relation to the processing of personal data carried out by the Department of Employment Affairs and Social Protection in connection with the Public Services Card, Appendix III of the DPC's 2019 Annual Report: www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf.

should exercise its formal powers under the 2018 Act and the GDPR. However, even where a complaint has been resolved amicably — i.e. to the satisfaction of the complainant — the making of the complaint might have brought wider or systemic compliance issues within the data controller/processor organisation to the attention of the DPC. Where the DPC has been alerted to such issues, it has a range of other audit and investigatory powers at its disposal outside of the complaint-handling mechanisms under the 2018 Act (for example, it can open an inquiry of its own volition into the issues or conduct an audit) to further address the core issues identified.

The rules of natural justice will apply so that the DPC must act fairly and impartially in investigating complaints etc.

Fair procedures in the context of a data protection investigation arose in the High Court case, Shatter v Data Protection Commissioner.[28] There, the DPC had issued a decision which found the former Minister for Justice had breached the data protection rights of another member of the Irish parliament. In coming to this conclusion, the DPC placed some reliance on an internal police email. The DPC had been shown the email but had never received a copy and had not furnished the Minister with a copy either. The High Court held:

> 43. Fair procedures would require that, at least, a copy of this document would also be shown to [the Minister]. This was not done. As a result, [the Minister] was deprived of an opportunity to make any observations or submissions concerning this central piece of evidence in the complaint.

Question 11

As noted above, there are currently 61 statutory inquiries underway examining matters of compliance under the GDPR and the LED as transposed, including 19 GDPR inquiries relating to international tech companies. The first wave of decisions, and corrective actions – where there are findings of infringements – arising from these inquiries was expected in the final quarter of 2019.

Question 12

No. The Data Protection Act 1988-2003 (as amended) did not provide for an award of damages for intangible harm. A plaintiff would have to establish material loss in order to succeed in an action for damages under those Acts.

28 [2017] IEHC 670.

A 2013 case, Collins v FBD Insurance p.l.c,[29] clarified the position that claimants would have to establish material loss in order to recover damages under the 1988-2003 Acts.

Question 13

Section 117(7) of the 2018 Act mirrors the GDPR and provides that a data protection action may be brought on behalf of a data subject by a not-for-profit body, organisation or association. In practice, Irish law does not currently provide for "class actions". However, a representative action as provided for by section 117 may be brought.

At the time of writing, there have been no Court decisions on any section 117 actions. Nor have data cooperatives or unions emerged at this stage.

However, privacy advocacy groups are active in Ireland and have brought actions in the public interest under the pre-GDPR regime. Notably, Digital Rights Ireland have taken a number of actions, one of which resulted in the judgment in *Digital Rights Ireland* wherein the Data Retention Directive was invalidated.[30]

Question 14

The DPC considers that cross-sectoral regulatory engagement is a vital aspect to the effective protection and vindication of individuals' rights as users of digital services. The DPC maintains close engagement with a range of domestic regulators, including with other competent authorities under the 2006 Regulation.[31]

The updated Consumer Protection Regulation (Regulation 2017/2394)[32] came into operation in January 2020, replacing the 2006 regulation, under which the DPC has been a competent authority for the purposes of co-operation regarding the E-Privacy Directive since 2009. Under the new Regulation, competent authorities are able to request the exercise of enforcement powers by other competent authorities. There are also provisions which allow for coordinated actions across member states, which may involve the Commission in some circumstances. It is likely that the DPC will continue to be the competent authority for the purposes of ePrivacy matters.

29 [2013] IEHC 137.

30 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*.

31 Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) [2004] OJ L364/1.

32 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 [2017] OJ L345/1.

The DPC also engages with other regulators in EU member states, and beyond, both on specific issues and more generally. In addition, the DPC participates in the Digital Clearing House – a cross-regulatory initiative established by the European Data Protection Supervisor bringing together regulators in the digital space (especially data protection, consumer law and competition law) and aimed at increasing co-operation and coherence, and deepening synergies between regulators.

The 2018 Act specifically recognizes the importance of collaboration between regulators/ other statutory bodies at both domestic and international level by way of Section 26 which creates an exemption from the general prohibition on the disclosure of confidential information by staff/ officers/Commissioners of the DPC, where such disclosure is made "to a public authority, whether in the State or otherwise, for the purposes of facilitating cooperation between the Commission and such authority in the performance of their respective functions".

D Data Processing for National Security Purposes

Question 15

The Explanatory Memorandum to the 2018 Act notes that while National Security and defence lie outside the scope of EU law, the Council of Europe's 1981 Data Protection Convention (Convention 108) is relevant to data processing for the purposes of safeguarding national security, defence and international relations in States that have ratified the Convention. The Data Protection Acts 1988 and 2003 (which amongst other things gave effect to the State's obligations under Convention 108 and transposed the Data Protection Directive into Irish law) have been largely repealed as of 25 May 2018 by the 2018 Act (save that they apply to certain types of processing and legacy - pre-25 May 2018 - complaints and investigations). One of the purposes for which that previous legislative regime has been retained relates to the processing of personal data for the purposes of safeguarding the security of the State, the defence of the State or the international relations of the State. Accordingly, complaints, contraventions and the obligations of relevant controllers in this sphere are found in the Data Protection Acts 1988 and 2003 rather than in the 2018 Act.

The meaning of "national security" within the context of data protection law received some consideration in the judgment of the High Court in Data Protection Commissioner v. Facebook Ireland Ltd.[33] In particular, in response to Facebook's argument that EU law

33 [2017] IEHC 545.

was not engaged insofar as the case concerned processing for national security purposes, the Court held *inter alia* at para. 61:

> … (4) This case is concerned with processing consisting of the transfer of data by a private company from a Member State to a private company in a third country. Thereafter, the data may be processed in the third country, the United States, for the purposes of national security, counter-terrorism and the prevention and detection of serious crime. The processing that arises for consideration is not solely the processing of data by the United States in its surveillance activities. Furthermore, the processing concerns commercial activities. This is not processing concerning public security, defence or state security. The parties to the transfers effected under the SCC decisions are private persons and companies, not State actors. The processing of the data by the United States subsequent to the transfer is unknown and uncertain. At the point of transfer it will not be known which data (if any) will be subject to surveillance. It follows that it cannot be said that the transfers concern public security or are for the purposes of national security. The argument is inconsistent with the case Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson & Ors (joined cases C-203/15 and C-698/15) (hereinafter "Watson"). The case concerned the interpretation of article 15 (1) of the Directive 2002/58/EC (the e-Directive). The legislation under review included measures adopted in Sweden and the United Kingdom for reasons of national security. The CJEU held that the national legislation fell within the scope of the e-Directive, notwithstanding article 1 (3) of that Directive which excluded from its scope "activities of the state" in specified fields, including activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State, when the activities relate to state security matters by analogy with the first indent of article 3 (2) of Directive 95/46. (see paras. 69 and 81).

It remains to be seen to what extent the CJEU will consider this issue in the context of the reference made by the Irish High Court to the CJEU in the proceedings taken by the DPC, concerning the validity of standard contractual clauses insofar as they apply to EU to US data transfers, which were heard before the CJEU in July 2019. The Opinion of the Advocate General in that reference case was delivered on 19 December 2019.

In addition, the judgment in Joined Cases C-203/15 and C-698/15, *Tele2 and Watson*[34] was applied in Dwyer v. Commissioner of An Garda Síochána[35] to the question of data retention for the purposes of combatting serious crime. The Irish data retention legislation (the 2011 Act) forced telecom providers to retain all telephony metadata for two years, and provided for disclosure to the Irish police force to prevent, detect, investigate or prosecute "serious" offences; safeguard national security; or save human lives. The plaintiff's challenge dealt only with the serious offences part of the framework.

In its ruling, the High Court agreed that aspects of the 2011 Act governing retention and disclosure of telephony data contravened EU law (other than where the mobile phone data was needed for national security or to save a human life) as they allowed for inappropriate, unnecessary or disproportionate use of data.

The Court disagreed with the State's argument that the judgment in *Tele2 and Watson*[36] should be interpreted narrowly, and that the Irish framework was acceptable under the CJEU's definition of "general and indiscriminate" retention. The Court said that position was difficult to reconcile with the conclusions of the CJEU which clearly state that the objective of fighting serious crime cannot in itself justify legislation providing for general and indiscriminate retention of data.

The Court refused to rule that the legislation's retention obligations were incompatible with the ECHR. The ECtHR has yet to rule on whether general and indiscriminate retention is compatible with the Convention, the Court noted, finding that the Court could therefore not declare the regime to be incompatible with the ECHR.

However, the Court held that the legislation's data access provisions violated the ECHR and EU law, as it set out no prior judicial or independent administrative review for telephony data access, and inadequate legislative guarantees against abuse.

The case was appealed to the Supreme Court and the judgment was delivered on 24 February 2020.

34 Joined Cases C-203/15 and C-698/15, *Tele2 and Watson.*

35 [2018] IEHC 685. Further background on this case is set out in response to Question 2 above.

36 Joined Cases C-203/15 and C-698/15, *Tele2 and Watson.*

Italy

Francesco Rossi Dal Pozzo[*]

A Setting the Scene

Question 1

Article 13 of Law 163/2017 mandated the Italian government to issue one or more legislative decrees to adapt the national regulatory framework to the provisions of Regulation (EU) 2016/679, the General Data Protection Regulation (hereinafter "GDPR").[1] Within this framework, Legislative Decree 101/2018 amending the Legislative Decree 196/2003 (hereinafter the "Personal Data Protection Code") was adopted.[2]

The new articles from 2-*ter* to 2-*septiesdecies* of the Personal Data Protection Code deal with the subjects expressly delegated by the GDPR to the national standard. These rules govern the processing of particular categories of data (personal data carried out for implementing a task of public interest or related to the work of public authorities, health data, child data, data relating to criminal sentencing and criminal offences) and dictate restrictions on the rights and obligations of the GDPR for judicial reasons, national security and public interest.

In particular, article 2-*quater* ensures that the Italian Data Protection Authority (Garante per la protezione dei dati personali, hereinafter, the "Italian Authority" or the "Authority") promotes the adoption of Codes of conduct for services provided for by articles 6(1)(c), 9, 86-90 GDPR.

These Codes of conduct cover: (i) processing and freedom of expression and information (article 85 GDPR); (ii) necessity of the processing to comply with a legal obligation to

* Professor of European Union Law, University of Milan, Italy.

1 Respectively, Law 163/2017, in *GURI*, 6 November 2017, No. 259 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Leg. dec. 101/2018, in *GURI*, 4 April 2018, No. 205. Leg. dec. 101/2018 is divided into six chapters and consists of 28 articles, dedicated to specific aspects of subject: Chapters I to IV (arts 1 to 16), with novelistic technique make the Code the necessary changes to ensure its compliance with the GDPR, repealing the incompatible provisions, amending others and inserting in some cases new provisions for implementing the regulatory reserves provided by the GDPR (see par. 2.1.1); chapters V and VI, on the other hand, cover the extra-codicist part of the regulatory intervention.

which the controller is subject (article 6(1)(c) GDPR); (iii) processing and public access to official documents (article 86 GDPR); (iv) processing of the national identification number (article 87 GDPR); (v) processing in the context of employment (article 88 GDPR); (vi) processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (article 89 GDPR).

In addition, article 45-*bis* of the Personal Data Protection Code states that the provisions contained in the new Part II implement the restrictions of article 23 GDPR about the processing necessary to fulfil a legal obligation or to carry out a task of public interest or related to the work of public authorities.

The Italian Authority has implemented the instruments of regulatory flexibility through the adoption of ethical rules that replaced the previous codes of ethics and good conduct (annexes A.1, A.2, A.3, A.4, A.6 of the former Personal Data Protection Code) as per the combined provisions of articles 2-*quater* of the Personal Data Protection Code and 20(4), of the Legislative Decree 101/2018. These rules, submitted by the Italian Authority to a compatibility review with Regulation (EU) 2016/679, were published in the Italian Official Journal, under the name of "Codes of conduct" and reported in annexe "A" of the Personal Data Protection Code.[3] As a result, their violation entails the application of the administrative penalty referred to in article 83(5) of the GDPR, and article 166 of the Personal Data Protection Code.

Furthermore, the Italian Authority has adopted detailed requirements concerning the processing of particular categories of data referred to in articles 6, 9 and 86-90 GDPR.[4]

3 Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities, provision 491/2018, in *GURI*, 4 January 2019, No. 3; Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system, provision 514/2018, in *GURI* 11, 14 January 2019, No. 11; Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes, provision 515/2018, in *GURI*, 14 January 2019, No. 11; Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations, provision 512/2018, in *GURI*, 15 January 2019, No. 12; Code of conduct and professional practice Regarding the processing of personal data For historical purposes, provision 513/2018, in *GURI*, 15 January 2019, No. 12.

4 Provision of 5 June 2019, containing the requirements relating to the processing of particular categories of data, under article 21(1) of leg. dec. 101/2018, in GURI, 29 July 2019, No. 176. In specific terms, these requirements include: (i) the processing of particular categories of data in employment reports (general authorisation of 1/2016); (ii) the processing of particular categories of data by membership bodies, foundations, churches and associations or religious communities (general authorisation of 6/2016); (iii) the processing of particular categories of data by private investigators; processing of genetic data (general authorisation of 8/2016); (iv) the processing of personal data for scientific research purposes (general authorisation of 9/2016).

Question 2

The Italian legislation does not provide for specific rules for the implementation of articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter "Charter").[5] However, the updated article 1 of the Personal Data Protection Code ensures that personal data is processed "in respect of human dignity, rights and fundamental freedoms of the person". Therefore, it indirectly protects the rights provided by articles 7 and 8 of the Charter.

The Charter has influenced the Italian case-law on the relationship between the right to anonymity and the right of reporting.[6] Indeed, the Italian Supreme Court (Corte di Cassazione) – addressing the subject of confidentiality, under articles 8 and 10(2) of the European Convention of Human Rights (hereinafter "ECHR") and articles 7 and 8 of the Charter – stated that the right to anonymity, in certain circumstances, can be constricted in favour of the equally fundamental right to of reporting.[7] These circumstances include: 1) the contribution made by broadcasting the image or news pertaining to a debate in the public interest; 2) the actual and current interest in broadcasting the image or news; 3) the high degree of notoriety of the subject represented, for the role covered within the public life of a country; 4) the ways used to obtain and give information, which must be truthful, proportionate to the purpose of informing in the public interest, and free from insinuations or personal considerations; 5) prior information about the publication or transmission of the news or image, so as to allow the right to reply before the disclosure to the public.

5 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

6 Cass. civ., 22 November 2018 No. 30193; Cass. civ., 9 August 2017, No. 19761; Court of Appeal, 24 June 2016, No. 13161; Cass. civ., 26 June 2013, No. 16111; Cass. civ., 5 April 2012, No. 5525. The Italian Constitutional Court No. 20/2019, in *GURI*, 27 February 2019, No. 9.

7 Cass. civ., 20 March 2018, No. 6919. Cass. civ. and 5 November 2018, No. 28084 which referred to the United Sections, the question of balancing the right to comment – intended to at the service of the public interest – and the right to be forgotten.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Fair processing

Concerning the principle of "fair processing", the monitoring activity by the Italian Authority was mainly dealing with the phenomenon of wild telemarketing.[8] In this context, the Italian Authority has made numerous requests for information to telephone operators (articles 157 and 158 of the Personal Data Protection Code) to acquire evidence to verify their approach in order to ensure the correct processing of the data of the data subjects. Therefore, the Italian Authority has ascertained several violations of the principle of fairness provided by Legislative Decree 196/2003.[9]

In addition, in February 2018, the Authority initiated proceedings against the Italian Democratic Party following individual reports complaining of the sending of political propaganda text messages in violation of the principle of fair processing.[10]

Furthermore, the Authority, by stating its opinion on the text "Update 2018-2019 of the National Statistical Programme 2017-2019", has informed the Parliament that in the context of the processing of data for statistical purposes it is necessary to provide the parties concerned with all the information referred to in articles 13 and 14 GDPR.[11]

Lastly, the Regional Administrative Court for Lazio has specified that the possible unlawful collection or mismanagement of data present on a platform, constitutes a possible violation of the principles of correct management of personal data, for which the Data Protection Authority is responsible for investigating.[12]

Purpose limitation

As part of its advisory activity, the Authority intervened on the concept of "purpose limitation". In particular, it issued a favourable opinion on the Framework Convention scheme between the Italian Ministry of Economy and Finance and the company Soluzioni per il Sistema Economico S.p.A. (SOSE), since the Convention itself identified the data

8 In 2018 this monitoring activity was marked by the adoption of injunction orders for the total amount, limited to this sector, of 3,440,000 euro (decisions 18 January 2018, No. 16; 22 May 2018, No. 330; 5 July 2018, No. 412; 26 July 2018, No. 441; 29 November 2018, No. 493).

9 Dec., 8 March 2018, No. 140; dec., 31 May 2018, No. 368 and 369, with which the Authority has prohibited unlawful processing by a call centre operating as a subcontractor on behalf of telephone operators in the absence of a specific and informed consent of those concerned.

10 Dec., 10 January 2019, No. 3.

11 Dec., 9 May 2018, No. 271.

12 Tar Lazio, 7 May 2018, No. 5043.

made available by SOSE, in accordance with the principles of purpose limitation and retention, integrity and confidentiality.[13]

Furthermore, despite the contrary opinion expressed by the Authority, the decree amending the discipline on the criminal record (Legislative Decree 122/2018) ruled out death as a reason for the cancellation of the registration in the criminal record, thus violating the principles of proportionality and purpose limitation referred to in article 5 GDPR and article 3 of the Legislative Decree 51/2018.

In addition, the Italian Supreme Court ruled on the judgement of legitimacy (*i.e.* the correct application of the law), establishing that the appeal to the Supreme Court containing a request for reduction of the penalty imposed by the Authority on the basis of the assessment of objective elements of the conduct and the purpose of the data processing is inadmissible, as it involves a new question which requires investigation of the facts.[14]

In its jurisdiction, the Court of Cagliari upheld the appeal made by a company against the Authority's order which had wrongly ascertained the disproportion between the processing of the data and the purpose of the data processing.[15] In the Court's view, the Authority's order made it very difficult for the applicant to carry out an activity which ensures the respect for fundamental rights and constitutional values, including social dignity (article 3 of the Constitution of the Italian Republic), scientific research (article 9 of the Constitution of the Italian Republic) and the right to health (article 32 of the Constitution of the Italian Republic).

Data minimisation

The principle of data minimisation has been widely applied in the context of civic access to Public Administration documents. In this regard, the Authority has stated that the display of personal data must not lead to an unjustified and disproportionate interference in the rights and freedoms of the persons to whom such data refer.[16] In accordance with the principle of minimisation, the Authority has also ordered a ban on the processing of data relating to employees through the use of vehicle tracking systems.[17]

The Supreme Court dealt with a case concerning the conduct of employees and data minimisation and ruled that employees must comply with the principle of data minimisation, according to which any person authorised for the processing must have access only to the personal data for which they have been authorised since they relate to

13 Dec., 26 July 2018, No. 439.
14 Cass. civ., 11 May 2018, No. 17278.
15 Court of Cagliari, 6 June 2017, No. 1569.
16 Dec., 20 December 2018, No. 518; dec., 24 December 2018, No. 519; dec., 11 October 2018, No. 464 and dec., 19 December 2018, No. 517.
17 Dec., 28 June 2018, No. 396 and 19 July 2018, No. 427.

the performance of their duties.[18] In the case at hand, an employee of a bank was transmitting the data of a customer to a colleague, in breach of his authorisation.[19]

Question 4

In light of the Italian Supreme Court's interpretation, consent (article 23 of the Personal Data Protection Code) is validly provided only if it is freely expressed and if it is clearly linked to a specific and identified processing.[20] Therefore, a website which provides fungible services can legitimately condition the provision of its services to the processing of data for advertising purposes, provided that the consent is individually given and linked to the specific purpose. However, the Italian Supreme Court considered that newsletter services dealing with finance, taxation, law and employment, which influence consumers by sending news under a general consent to receive "promotional information" violated consumers' privacy. In addition, the Italian Supreme Court interpreted the relationship between freedom of information and the consent of claimants, stating that TV broadcasters must pay compensation for damages resulting from the violation of privacy due to the broadcasting of a TV report without the consent of the person filmed, whose sensitive data are shared.[21]

There are no relevant judgments as to the legitimate interest of the data controller.

Question 5

The issue has been widely debated at national level. The Big Data fact-finding survey, jointly launched by the Italian Competition Authority (hereinafter AGCM), the Communications Regulatory Authority (hereinafter "AGCom") and the Data Protection Authority, shows that data is collected through increasingly complex and innovative technologies to extract an informative value.[22] The authorities noted that the transfer of personal data for the use of free web services is implicit, *i.e.* not contractual. This implicit business relationship is based on the lack of economic compensation, since the market, missing a regulatory framework on the trade of data, does not assign any price to the transaction.

18 Cass. pen., 8 January 2019, No. 565.

19 In infringement of article 615-*ter* of the Italian Criminal Code.

20 Cass. civ., 2 July 2018, No. 17278.

21 Cass. civ., 21 June 2018, No. 16358; see also the Court of Turin (27 February 2019, No. 940) that has also recently expressed its opinion that, without the consent of the claimants, any broadcasting of the image of known persons is prohibited if it does not respond to social usefulness; Court of Milan, 12 February 2019, No. 1355.

22 The joint inquiry on "Big data" launched by the AGCOM deliberation No. 217/17 / CONS.

In addition, the recent "policy guidelines and recommendations" have specified that information asymmetries between users and digital operators *must be reduced in data collection*.[23] To this end, the synergy between the personal Data Protection legislation and the consumer protection reduces this information asymmetry by ensuring that users receive "adequate, timely and immediate information about the purpose for collecting and using their data".

Question 6

With regard to the implementation of article 22 GDPR, Legislative Decree 51/2018 is particularly important.[24] The Decree provides an organic protocol for the processing of personal data carried out for the purposes of prevention, investigation, detection and prosecution of criminal offences or execution of criminal penalties. In particular, article 8 of Legislative Decree 51/2018 provides for the prohibition of decisions based exclusively on automated processing, including profiling, which produce negative effects on the data subject. Automated processing authorised by EU law or by specific legal provisions are exempted. However, adequate guarantees must be ensured for the data subject's rights and freedoms, including the right of the data subject to obtain the human intervention of the data controller. Furthermore, article 2-*octies* of the Personal Data Protection Code establishes the principles for the processing of data relating to criminal convictions and offences. Specifically, the provision states that, except the cases provided for by Legislative Decree 51/2018, the processing of personal data relating to criminal convictions outside the control of the public authority is only permitted in the specified areas (article 2-*octies*(3)), if it has been previously authorised by laws or regulations that provide for appropriate guarantees of the rights and freedoms of the data subjects (article 2-*octies*(1)). In the absence of such provisions, the processing operations and related guarantees are identified by decree of the Minister of Justice, pursuant to article 17(3) of the Law 400/1988, after consultation with the Authority (article 2-*octies*(2)).

Last, articles 2-*undecies* and 2-*duodecies* of the Personal Data Protection Code restrict rights and obligations provided by articles from 12 to 22 GDPR, for judicial reasons.

23 Big data Interim report 2018 and Big Data: Policy Guidelines and Recommendations of 2 July 2019 in the context of the joint inquiry on "Big data" launched by the AGCOM deliberation No. 217/17 / CONS.

24 Leg. dec., 18 May 2018, No. 51, in *GURI*, 24 May 2018, No 119, on the Implementation of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

Among the guarantees, chapter II of Decree 51/2018, under the heading "Rights of the data subject", provides for the obligation of the data controller to inform the data subject of the information referred to in articles from 10 to 14 and 27, so that he can exercise his rights to access, rectify, cancel and complain to the Authority or to file a judicial appeal (article 9).

In addition, article 21 stipulates that the collection, modification, consultation, communication, transfer, interconnection and deletion of data, performed in automated processing systems, must be recorded in dedicated *log* files, to be kept for the period established by decree of the President of the Republic, adopted pursuant to article 17(1) of the Law 400/1988. Article 25 of Decree 51/2018 establishes an obligation for the data controller and the data processor to implement technical and organisational measures to ensure an appropriate level of security for the risk of data breach, balancing technical knowledge, implementation costs, nature, object, context and purpose of the processing, as well as the degree of risk for the rights and freedoms of individuals.

Excluding the cases governed by that decree, articles 2-*undecies* and 2-*duodecies* of the Personal Data Protection Code stipulate that the exercise of the rights of the data subject may be delayed, restricted or excluded. However, that limitation must be communicated, without delay, to the data subject, unless such communication could compromise the purpose of the limitation, for the time and to the extent that it constitutes a necessary and proportionate measure, considering the fundamental rights and legitimate interests of the data subject.

Question 7

Since the application of the GDPR, there has been an increase in the number of requests to obtain the updating or removal of data which, initially processed lawfully, due to a change in the situation or the passage of time, are subject to the "right to be forgotten" discipline.[25] This right is intended as a dynamic projection of the person's right not to remain indefinitely exposed to further damage to his honour and reputation that may result from the repeated publication of news legitimately disclosed in the past.

In this context, the Authority's efforts focused on complaints about the removal of URLs addressed to various search engines (Bing, Yahoo, Virgil and, especially, Google Inc.), considering prevailing, in most cases, the interest of the public to have access to the controversial information.[26] Conversely, the Authority, where it considered that the public interest was recessive with respect to the right to honour, accepted the complaint of the

25 Judgement of 13 May 2014 in Case 131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Google Spain), [ECLI:EU:C:2014:317].

26 Dec., 13 December 2018, No. 503; dec., 13 December 2018, No. 505; dec., 13 December 2018, No. 506.

data subject by inhibiting the disclosure of personal data.[27] The Court of Lucca has ruled that the so-called "right to be forgotten" should be excluded if a short interval has elapsed between the facts from which the case originated and the final moment of the case itself, which is undeniably insufficient to weaken the collective interest in knowledge and disclosure.[28] This decision is consistent with the previous decision of the Italian Supreme Court according to which the protection of the right to be forgotten must also be assessed with reference to the time of storage of personal data in public records.[29]

With regard to the relationship between the Authority and the ordinary jurisdiction, the Court of Milan overturned an Authority's order stating that the defamatory nature of the contested links must be examined by the ordinary judge who is responsible for balancing the right to honour or reputation and the right to freedom of expression of thought.[30] Last, the Court of Milan – in the proceedings in which the Authority opposed Yahoo Emea Limited, starting from the assumption that the search engine is the data controller and not a mere intermediary – ruled that any real and effective activity, even minimal, exercised by them through a permanent organisation, is relevant to the jurisdiction of the Italian court.[31]

Question 8

Article 12 of Legislative Decree 101/2018 – in implementation of article 85 GDPR – provides for amendments to Title XII (articles 136 to 139) of the Personal Data Protection Code, the heading of which has been replaced in "Journalism, Freedom of Information and Expression", whose provisions apply both to the processing carried out in the exercise of the profession of journalist and to the processing aimed exclusively at the publication or dissemination, even occasional, of articles, essays and other manifestations of thought, including academic, artistic and literary expressions.

In addition, pursuant to article 2-*quater* and 139 of the Personal Data Protection Code, the Authority promotes the adoption by the National Council of the Order of Journalists of rules of conduct that, relating to the processing of data under article 136, provide for measures to protect the data subject, differentiated on the basis of the nature of the data. In this regard, pursuant to article 20(4) of the Legislative Decree 101/2018, the Authority

27 Dec., 26 October 2017, No. 444; dec.,16 November 2017, No 487; dec., 7 February 2019, No. 38.

28 Trib. Lucca, 19 January 2019, No. 96.

29 Cass. civ., 20 March 2018, No. 6919; Cass. civ., 22 November 2018, No. 30193; Cass. Civ., 9 April 1998, No. 3679; Cass. civ., 9 August 2017, No. 19761.

30 Court of Milan, 5 September 2018, No. 7846 overturned the Italian Data Protection Authority's order of Dec., 21 December 2017, No. 557.

31 Respectively, Court of Milan, 22 January 2018, No. 491 and the Italian Data Protection Authority's order of Dec., 26 January 2017, No. 30.

has verified the compatibility of the code of ethics of journalists with the GDPR.[32] As part of this verification, the Authority has identified provisions deemed compatible with the GDPR in order to have them published in the Official Journal under the new name of "Rules of conduct relating to the processing of personal data in the exercise of journalistic activities." These rules of conduct have been listed in annex A of the Personal Data Protection Code in place of the previous Codes of conduct.[33] Therefore, the new provisions constitute essential conditions for the legality of the processing of data in the journalistic field, as provided for in the combined provisions of articles 2-*quater*, 102 and 136-139 of the Personal Data Protection Code.

The Authority has addressed numerous interventions related to the interaction between freedom of expression of thought and potential violations of the right to privacy by the media. In this regard, the Authority has adopted, as a matter of urgency, some measures to limit the further dissemination of television reports and articles containing detailed information suitable for identifying, albeit indirectly, the victims of sex crimes.[34] In some cases, on the other hand, the reasons of the data subject have been considered recessive with respect to the right of information: this is the case with press articles concerning the criminal record of persons carrying out professional activities of public importance.[35]

The freedom of expression of thought has been subject to some interventions by Italian judges. The Italian Supreme Court has ruled that - pursuant to article 137(2) of Legislative Decree 196/2003 - the processing of personal data for journalistic purposes may be carried out without the consent of the data subject.[36] However, such processing must include procedures that ensure respect for fundamental rights and freedoms, the dignity of the data subject, the right to personal identity, and the code of conduct of journalists, which is a regulatory source pursuant to article 139 of Legislative Decree 196/2003. Moreover, the relevant case-law has established that the presence of the conditions legitimising the exercise of the right of reporting does not exhaust, in itself, the analysis of the legitimacy of the publication or broadcasting of the image of the persons involved.[37] To this end, the public interest in the knowledge of a certain news must first be distinguished from the autonomous and specific public interest in the knowledge of the appearance of the protagonists of the narrated event. In the second case, the precautions that surround the

32 Dec., 29 November 2018, No. 491.

33 Min. Dec., 31 January 2019, in *GURI*, 11 February 2019, No. 35.

34 Dec., 29 November 2018, No. 486, 487, 488, 489 and 490.

35 Dec., 13 December 2018, No. 505 and No. 506.

36 Cass. civ., 9 July 2018, No. 18006. The Supreme Court upheld the judgement as to the merits which ruled that the journalist had to compensate the damages arising from the unlawful disclosure of a recorded conversation without the person's knowledge, in violation of Art. 2 of the Journalists' Code of conduct.

37 Court of Lucca, 19 January 2019, No. 96.

diffusion of the image, due to the greater offensive potential of the visual instrument, must be more stringent.

C Domestic Enforcement of Data Protection Law

Question 9

The Italian Data Protection Authority is established by the so-called Privacy Act of 1995.[38]

Article 2-bis of the Personal Data Protection Code, as amended by Art. 14 of the Legislative Decree 101/2018, entrusts the Authority with the task of implementing the provisions of the Personal Data Protection Code and the GDPR, as well as to supervise their proper observance, regulating how they operate in accordance with the principles and in harmony with other rules in force. The Personal Data Protection Code regulates: (i) the organisation chart and the organisational structure (article 153); (ii) the requirements and procedures for the choice of employees, as well as the tasks and emoluments due to them (articles 153, 155 and 156); (iii) tasks and powers (articles 154 and 154-*bis*); (4) the measures which it may enact, with the express exclusion of its intervention in relation to the processing of data carried out by the judicial authorities in the exercise of their functions (articles 157 and 158). Finally, the Authority is entitled to act and to be in Court through professionals of the State Attorney's Office, its own qualified employees or further lawyers (article 154-*ter*).

The first report on the application of the GDPR in Italy, which refers to the period between 25 May and 31 March 2019, lists 48,591 communications of the contact details of the Head of Data Protection (article 37(7) GDPR and article 28(4) of the Legislative Decree 51/2018), 7,219 reports and complaints, 946 notifications of Data Breach and 18,557 contacts with the Public Relations Office.[39]

38 Law, 31 December 1996, No. 675, in *GURI*, 8 January1997, No. 5; the law has been repealed under Art.183, para. 1, a), of the Personal Data Protection Code.

39 See GDPR Application Budget (25 May 2018 – 31 March 2019) published by the Italian Data Protection Authority, [www.garanteprivacy.it/documents/10160/0/REGOLAMENTO+UE++Il+bilancio+di+applicazione+dal+25+maggio+2018+al+31+marzo+2019.pdf/a9697ab0-d107-fe2f-53e1-6883ec0bd25e?version=1.2], visited 28 July 2019.

Question 10

The Personal Data Protection Code provides that the data subject has the right to lodge a complaint (article 141) and may address a report (article 144) to the Authority who governs the respective proceedings with its own regulations (article 142(5)). In this regard, the Authority, by resolution of 4 April 2019, adopted Regulation 1/2019, relating to the procedures for examining the complaints and reports.[40] Specifically, chapter I of Regulation 1/2019, entitled "Procedures concerning protection before the Authority", consists of two sections governing complaints and reports respectively. More in detail, the first section regulates complaints, *i.e.* acts indicating the elements provided for by article 142 of the Personal Data Protection Code, including the detailed indication of the facts and circumstances on which it is based, the provisions which are presumed to have been violated, the measures requested and the documentation useful for its evaluation (article 8). Specific provisions are also provided for in relation to the various phases of the procedure for examining the complaint, such as the processing (article 9), the preliminary investigation (articles 10 and 11) and the decision (articles 14 to 18).

The reports are identified instead with the residual category of acts originating by anonymous complaints, which, different from the requests for opinion, questions and complaints, are directed to solicit a control by the Authority on the relevant discipline in relation to personal data processing (article 19(1)). The second section also provides that the Authority may use the information indicated in the reports if it deems it necessary to start controls on cases in which it sees the risk of serious prejudice or retaliation to the detriment of subjects concerned by the processing, or for cases of particular gravity (article 19(2)).

Although the report can be examined by the Authority for the purposes of verification of a possible breach, this does not involve the necessary adoption of a measure (article 19(3)). In fact, the Authority can conclude the examination of the report by arranging its filing when one of the conditions set out in article 11(1) occurs, or in the case of completely generic reports, or limited to imputing to a subject facts which do not contain any circumstantial evidence or elements that allow for the data controller to be easily identified (article 19(5)). If the report is not filed under article 19(5), the Authority may initiate the preliminary investigation and the administrative procedure for which the provisions for complaints in articles 9 to 18 are observed (article 20).

The law has inserted in the Data Protection Code a new Chapter 0.1 entitled "Alternativeness of the forms of protection" which consists of a single article 140-*bis* "Alternative Forms of Protection". This provision, given that articles 77 and 79 GDPR do not prejudice the possibility of availing of any other available administrative or extra-judicial

40 Regulation 1/2019, in *GURI*, 8 May 2019, No. 106.

recourse, confirms the referral of the choice to the data subject to lodge a complaint to the Authority or appeal to the Judicial Authority if he considers that the rights he enjoys on the basis of the regulations on the protection of personal data have been violated, safeguarding the rule of the alternativeness of judicial protection with that before the Authority. This applies only to cases proposed for the same subject and between the same parties, to avoid duplication of proceedings with the risk, in case of an appeal of the Authority's decision, of a potential conflict of "judgements".

In addition, it is appropriate to recall the instruments for regulating complaints, reports and requests for preliminary verification pursuant to articles 18 and 19 of the Legislative Decree 101/2018. These provisions introduced, respectively, the procedure of facilitated definition of the violations in matters of protection of personal data and the handling of past business. In the first case, starting from 19 September 2018, offenders were given the faculty to define, on a facilitated basis, the sanction procedures concerning the violations referred to in articles 33, 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*(2), which were not, at the date of application of the GDPR, already defined with the adoption of the injunction-order.

This procedure of facilitated definition registered a scarce adhesion by the subjects involved, leading to the definition of the aforementioned 88 sanctioning proceedings and to the subsequent collection of a total amount of 386,400 euro. With regard to the handling of past business, it was provided that, by 4 December 2018, the data subjects could submit a request to the Authority for handling complaints, reports and requests for preliminary verifications relating only to the institutions governed by the Data Protection Code prior to the amendments made to it by the application of the GDPR. This interpretation was based, on the one hand, on the fact that the right to file complaints or reports based on the new regulations could not be waived (article 77 GDPR; articles 141 to 144 of the Personal Data Protection Code, as amended by the Legislative Decree 101/2018), prevailing over any conflicting internal sources, and on the other hand, on the fact that, following the date of application of the GDPR, the institution of the preliminary verification was incompatible with the Regulation itself.[41]

Question 11

One of the most relevant aspects of Legislative Decree 101/2018 is the system of sanctions, not only for its evident centrality in the new European Data Protection regulation, but also because the system of referrals to the various regulatory provisions contained therein

41 Dec., 27 September 2018, No. 455, in *GURI*, 4 October 2018, No. 231.

(including those of Legislative Decree 196/2003 which the law did not repeal) involves difficulties of interpretation.

By virtue of the faculty provided by article 84 GDPR, Legislative Decree 101/2018 has made significant changes to Part III, Title III of the Personal Data Protection Code. In particular, pursuant to article 15(3) of the Legislative Decree 101/2018, the Authority is the competent body to impose the administrative pecuniary sanctions referred to in article 166 of the Personal Data Protection Code. In this regard, in 2018, the Authority started 707 administrative sanctioning proceedings, whose acts were adopted on the basis of the previous discipline under Law 689/1981, as referred to in the Personal Data Protection Code before the entry into force of Legislative Decree 101/2018.[42]

All these sanctioning proceedings, including those initiated after the GDPR's application date, concern the ascertainment of violations that occurred before 25 May 2018, *i.e.* at the time when the Personal Data Protection Code was in force in its formulation prior to the amendments introduced by Legislative Decree 101/2018. Therefore, by virtue of the principle *tempus regit actum*, these violations were challenged according to the procedure provided for by the aforementioned Law 689/1981. With regard to the measures issued under the new legislation, excluding those concerning the Rousseau Association, Tim S.p.A. and Eni Gas e Luce S.p.A., the Authority did not impose any relevant pecuniary sanction.[43]

With regard to criminal penalties, the GDPR allows Member States to lay down the provisions relating to them. Therefore, the Data Protection Code, as amended and integrated by Legislative Decree 101/2018, regulates the criminal cases relating to: unlawful processing of data (article 167); unlawful communication and dissemination of personal data subject to large-scale processing (article 167-*bis*); fraudulent acquisition of personal data subject to large-scale processing (article 167-*ter*); falsity in the declarations made to the Authority and interruption of the execution of the tasks or the exercise of the powers of the Authority itself (article 168); non-compliance with the provisions issued by the Authority (article 170).

42 Law, 24 November 1981, No. 689, in *GURI*, 30 November 1981, No. 329.

43 For the measures issued under the new legislation *see* Dec., 4 April 2019, No. 90; 18 April 2019, No. 96; 30 April 2019, No. 106; 29 May 2019, No. 121; 5 June 2019, No. 125;12 June 2019, No. 130; 20 June 2019, No. 137 and 20 June 2019, No. 141. For the measure concerning the Rousseau Association Tim S.p.A. and Eni Gas e Luce S.p.A. see respectively Dec., 4 April 2019, No. 83; Dec., 15 January 2020, n. 7; Dec. 11 December 2019, n. 232.

Question 12

From a literal point of view, the Italian legal system does not recognise the dichotomy between "material damage" and "immaterial damage". However, these categories can be traced back respectively to the pecuniary and non-pecuniary damages provided by the Italian Civil Code. In this regard, in the opinion of the Supreme Court, non-pecuniary damages can be compensated only in the cases "provided for by the law", *i.e.,* according to a constitutionally oriented interpretation of Article 2059 of the Civil Code: (a) when the illicit act is abstractly configurable as a criminal offence; in such a case, the victim will be entitled to compensation for non-pecuniary damages arising from the injury of any interest of the person protected by the law, even if not of constitutional relevance; (b) when one of the cases in which the law expressly allows the compensation of non-pecuniary damages even outside of a crime hypothesis (*e.g.* unlawful processing of personal data) occurs; in this case, the victim will be entitled to compensation for the non-pecuniary damages resulting from the injury of the interests of the person whom the legislator intended to protect through the rule conferring the right to compensation (such as the right to confidentiality or not to suffer discrimination); (c) when the unlawful act has seriously violated the person's inviolable rights, as such an object of constitutional protection; in this case, the victim will be entitled to compensation for non-pecuniary damages resulting from the injury of such interests, which, contrary to the first two hypotheses, are not identified *ex ante* by law, but must be selected by the judge on a case-by-case basis.[44]

With regard to the conditions for compensation for damage, the sole circumstance that the data have been used by the controller or anyone else in an unlawful or incorrect manner does not legitimise the data subject to claim compensation for non-pecuniary damages. Indeed, the damage from violation of the fundamental right to the protection of personal data does not escape the verification of the seriousness of the injury and of the damage (as a personal loss actually suffered by the data subject). In fact, also with reference to this right, the balance is made with the principle of solidarity pursuant to article 2 of the Constitution of the Italian Republic, to which the principle of tolerance of the minimum injury is intrinsically linked. Therefore, a mere violation of the Personal Data Protection Code does not entail an unjustifiable violation of the right, but a significant offence should recur.

Moreover, the damages caused by the processing of personal data are subject to the discipline of article 2050 Italian Civil Code, with the consequence that the injured party is only required to prove the damage and the causal link with the activity of data processing, while it is up to the defendant to prove that he has taken all appropriate measures to avoid the damage.

44 Cass. Civ., 11 November 2008, No. 26972; Consiglio di Stato, 3 June 2014, No. 2844.

Therefore, the damage is to be attributed to those who have processed personal data or those who have used another party's processing unless they demonstrate that they have taken all the appropriate measures to avoid the damage *ex* article 2050 Civil Code. Furthermore, the non-pecuniary consequences of such damage - whether contractual or extra-contractual - are to be considered *in re ipsa* unless the party causing the damage proves that there has been no such damage or that the damage is insignificant or that the injured party has benefited from the publication of the data.[45,46]

Finally, concerning bank's unlawful reporting to the Crif (Center for Research in International Finance), the entrepreneur wrongly referred to as a bad payer, cannot have *de plano* the compensation for damages, but must prove it. The ascertained violation in the use of the customer's personal erroneously indicated by the bank does not relieve the customer from proving the damage to his reputation and offering means of proof to quantify it.

Question 13

Law 31/2019 reformed the institute of the class action by bringing its discipline within the Italian Code of Civil Procedure, to broaden its scope and strengthen it.[47] In particular, article 1 introduced into the Code of Civil Procedure the title VIII-bis called "Collective proceedings", composed of 15 new articles (from article 840-*bis* to article 840-*sexiesdecies*). The reform will enter into force on 19 April 2020, the date from which the provisions of the current consumer code and, in particular, article 140-*bis*, will cease to apply.

Implementing article 80 GDPR, article 142(2) of the Personal Data Protection Code provides that the complaint pursuant to article 77 GDPR is signed by the data subject or, on his behalf, by a third sector entity subject to the discipline of Legislative Decree 117/2017, which is active in the field of protection of rights and freedoms of data subjects, with regard to personal data protection.[48] The action for damages is governed by the aforementioned article 140-*bis* of the Consumer Code.

The most active third sector organisations include consumer associations (*e.g.*, Altroconsumo).

45 Cass. Civ., 8 January 2019, No. 207; Cass. civ., 4 June 2018, No. 14242; Cass. civ., 15.7.2014, No. 16133; Court of Appeal of Turin, 4 February 2019, No. 26; Court of Siena, 29 October 2018, No. 1244.

46 Cass. civ., 8 January 2019, No. 207.

47 Law, 12 April 2019, No. 31, Class Action Rules, in *GURI*, 18 April 2019, No. 92.

48 Leg. dec., 3 July 2017, No. 117, in *GURI*, 2 August 2017, No. 179.

Question 14

AGCM, AGCom and the Data Protection Authority launched a joint survey to identify possible issues related to the use of so-called *big data* and the definition of a framework of rules capable of promoting and safeguarding: the protection of personal data, the competition on the markets within the digital economy, the consumer protection and the pluralism in the digital ecosystem.[49] In particular, it has been observed that exploiting *big data*, even in relation to anonymous or aggregated data, can result in increasingly precise profiling, with the risk of new forms of discrimination and, more generally, of freedom restrictions. Therefore, through the joint investigation, the three Authorities intend to verify the impact of information aggregation and of *big data* accessibility obtained through non-negotiated forms of user profiling on the digital ecosystem.

D Data Processing for National Security Purposes

Question 15

According to the Italian Constitutional Court's judgment 86/1977, national security corresponds to the external and internal security of the state, that is, the need to protect the supreme interests that apply to any community organised in a State from any violent action or any other action contrary to the democratic spirit that inspires our Constitutional structure.[50]

In particular, articles 6 and 7 of Law 124/2007, respectively, define national security as defence of the independence, integrity and security of the Republic and internal security of the Republic and the democratic institutions set out in the Constitution of the Italian Republic from any threat, any subversive activity and any form of criminal or terrorist aggression.[51]

Title III "State Defence and Security", Chapter I of the Personal Data Protection Code provides for a single article: article 58 "Specific provisions for the processing of personal data for national security or defence purposes", which regulates that the processing of personal data carried out by the bodies of the Republic's Security Information System, *i.e.* data covered by State secrecy, must be in accordance with the provisions of article 160(4) of the Personal Data Protection Code, as well as of Legislative Decree 51/2018, insofar as they are compatible.

49 See footnote *n. 23*.
50 Corte Costituzionale, 24 May 1977, No. 86.
51 Law, 3 August 2007, No. 124, in *GURI*, 13 August 2007, No. 187.

In the implementation within Legislative Decree 101/2018, the Authority considered the new article 132 of the Personal Data Protection Code containing a waiver - introduced by article 24 Law 167/2017 - regarding the storage of telephone and traffic data in order to ensure the effectiveness of investigative tools in light of extraordinary needs of counter-terrorism, including international terrorism, as well as for the purposes of the investigation and prosecution of the offences referred to in article 51(3-*quarter*), and 407(2)(a) Italian Code of Criminal Procedure. In specific terms, the Authority noted that the confirmation of this waiver would have led to significant criticisms with respect to the principle of proportionality between investigative needs and limitations to the right to Data Protection of citizens affirmed by the Court of Justice of the European Union (hereinafter "CJEU") with the rulings *Digital Rights Ireland* and *Tele2*.[52] Because of the incompatibility of this waiver with the principle of proportionality (as interpreted by the CJEU) and in order to ensure full compliance of the national legislation with EU law, the Authority asked the Italian government to remove any reference to the aforementioned article 24 Law 167/2017, from the Decree. However, such instructions were not followed.

Moreover, the Italian Supreme Court recently expressed its opinion on the matter. In its view, pursuant to articles 8 of the ECHR and articles 7 and 8 of the Charter, the data subject is not entitled to the cancellation of data in public registers. It is legitimate to retain data when required by law and when it entails a measure necessary for national security, public safety, economic well-being of the country, prevention of disorder and crime, protection of health or morality and protection of third parties' rights and freedoms.[53]

52 Respectively, Judgment of 8 April 2014, in joined Cases 293/12 and 594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Digital Rights Ireland), [ECLI:EU:C:2014:238] and Judgment of 21 December 2016, in joined Cases 203/15 and 698/15, *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Tele2 Sverige AB), [ECLI:EU:C:2016:970].

53 Cass. civ., 9 August 2017, No. 19761.

Luxembourg

Tine A. Larsen, Clémentine Boulanger and Annelies Vandendriessche[*]

A Présentation du contexte

Question 1

La réponse à cette première question s'effectuera en deux temps. A titre liminaire, il s'agira d'identifier et de décrire les principaux instruments juridiques introduits en droit luxembourgeois pour mettre en œuvre le Règlement Général sur la Protection des Données (règlement 2016/679, ci-après le « RGPD ») (1) pour ensuite mettre en exergue les principales marges de manœuvres permises par le RGPD (2).

1) L'identification et la description des principaux instruments juridiques introduits en droit Luxembourgeois pour mettre en œuvre le RGPD

Le RGPD est directement applicable dans la législation luxembourgeoise. La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données (ci-après désignée « CNPD ») et du régime général sur la protection des données a abrogé la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Ladite loi confère un statut juridique à la CNPD, décrit les compétences de celle-ci, ses missions, ses pouvoirs, la composition, la nomination de ses membres et son fonctionnement. Le processus d'enquête et les décisions prises à l'issue de l'enquête y sont décrits, ainsi que la possibilité de la CNPD à imposer des amendes administratives.

In fine, la loi prévoit la création d'un Commissariat du Gouvernement à la protection des données auprès de l'Etat. Celui-ci est placé sous l'autorité du Premier Ministre. Il est chargé de « développer la protection des données à caractère personnel au sein de l'administration étatique, de promouvoir les bonnes pratiques à travers l'administration étatique et de stimuler la sensibilisation des agents; de contribuer à une mise en œuvre cohérente des politiques dans ce domaine ». Il peut également assurer la fonction de délégué

* Tine A. Larsen: Présidente de la Commission nationale pour la protection des données de Luxembourg (CNPD). Clémentine Boulanger: Conseillère Juridique auprès de la Commission nationale pour la protection des données de Luxembourg (CNPD). Annelies Vandendriessche: Chercheur en formation doctorale à l'Université du Luxembourg.

à la protection des données pour les chefs d'administrations compétents du ressort ou sous l'autorité des ministres ou encore celui des communes.

2) Mise en œuvre des principales marges de manœuvre permises par le RGPD à travers les instruments précédemment identifiés

a) Mise en œuvre de l'article 6(1)(c) du RGPD

La mise en œuvre de l'article 6(1)(c) du RGPD ne fait pas l'objet de spécificités en droit luxembourgeois.

b) Mise en œuvre de l'article 9(4) du RGPD

Le législateur luxembourgeois limite le traitement de données génétiques. En effet, l'article 66 de la loi du 1er août 2018 interdit le traitement de données génétiques en matière de droit du travail et d'assurance.[1] Une telle démarche s'inscrit dans la continuité puisque le législateur luxembourgeois prévoyait déjà dans la loi modifiée du 2 août 2002 transposant la Directive 95/46, des règles spécifiques au traitement des données génétiques, qui avaient été ajoutées par le législateur à la liste de données sensibles.[2]

c) Mise en œuvre des articles 6(2) et 23 du RGPD

L'article 23 du RGPD prévoit des limitations quant aux droits prévus aux articles 12 à 22 et l'article 34, ainsi qu'à l'article 5 du RGPD. Il y peut être observé que certaines de ces limitations sont prévues en droit luxembourgeois. En effet, la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale prévoit une limitation de la fourniture ou la non fourniture des informations à la personne concernée, limite le droit d'accès de cette dernière, limite le droit de rectification ou d'effacement des données et la limitation du traitement.

Un projet de loi a été introduit à la Chambre des Députés fin 2018[3] visant à limiter la portée de certaines obligations et droits contenus dans le RGPD sur base de l'article 23(2) RGPD. Le projet de loi, a pour objet de faciliter la surveillance macro prudentielle du secteur financier et du secteur des assurances au Luxembourg par la Commission de surveillance du secteur financier (ci-après désignée « CSSF ») et par le Commissariat aux Assurances (ci-après désigné « CAA ») et ce, dans les domaines relevant de la compétence

1 Pour plus d'informations sur ce point, J-L- Schiltz et M. Spielmann, 'Mondialisation et Internet' (2016) 26 Annales de Droit Luxembourgeois p. 133, p. 138.

2 *Ibidem*, art. 6; J-L Schiltz et M. Spielmann, *op. cit.* 2, p. 138.

3 Projet de loi N°7373 concernant la limitation de la portée de certains droits et obligations dans le cadre du RGPD.

du Fonds de résolution et du Fonds de garantie des dépôts. Des limitations aux droits de la personne prévus aux articles 13, 14, 15, 18 et 21 RGPD sont envisagés par ledit projet de loi.[4] Dans son avis la CNPD a souligné que le législateur doit fournir des motivations précises justifiant la nécessité et proportionnalité des limitations prévues aux fins d'intérêt public poursuivis par la CSSF et le CAA.[5]

Un autre projet de loi en cours vise à adopter des limitations aux droits prévus aux articles 15, 16 et 18 du RGPD en matière fiscale, également en vertu de l'article 23(2) RGPD.[6] Le but serait de limiter la portée de ces droits en respectant le principe de proportionnalité afin de ne pas entraver la procédure de collecte des impôts par l'Administration des contributions directes.[7] Ici encore, la CNPD a souligné dans son avis que les limitations adoptées en vertu de l'article 23(2) RGPD doivent respecter l'essence du droit fondamental à la protection des données.[8] A cet égard, la CNPD s'est révélée très critique quant au projet de loi, en affirmant que le projet de loi en question vide de son essence le droit fondamental de la protection des données en limitant les droits garantis par le RGPD dans leur ensemble.[9] Le projet de loi est actuellement renvoyé en commission parlementaire pour de plus amples débats.

d) Mise en œuvre de l'article 85 du RGPD

Le législateur a adopté des dérogations en vue de la protection de la liberté d'expression et d'information à l'article 62 de la loi du 1er août 2018, étant donné que l'adoption de telles exemptions et dérogations sont requises par l'article 85(2) RGPD.[10]

e) Mise en œuvre de l'article 86 du RGPD

La loi du 14 septembre 2018 relative à une administration transparente et ouverte a pour objet de définir un cadre pour la mise en œuvre d'une politique d'ouverture aux personnes physiques et morales vers les documents détenus par les acteurs mentionnés à l'article 1er paragraphe 1er de la loi.[11] Les documents pouvant être accessibles ou délivrés sont

4 Avis de la CNPD du 5.4.2019 – Projet de loi N°7373, pp. 2 & 3.
5 *Ibidem*, p. 4.
6 Projet de loi N° 7250 portant exécution, en matière fiscale, des dispositions du RGPD.
7 *Ibidem*, p. 4.
8 Avis de la CNPD du 29.3.2018 – Projet de loi N° 7250, p. 3.
9 *Ibidem*, p. 12.
10 Voir la réponse à la question 8.
11 Il s'agit en effet les administrations et services de l'Etat, les communes et les syndicats de communes, les établissements publics placés sous la tutelle de l'Etat ou sous la surveillance des communes, les personnes morales fournissant des services publics, la Chambre des Députés, le Conseil d'Etat, la Cour des comptes, les Chambres professionnelles.

exclusivement ceux relatifs à l'exercice d'une activité administrative desdits acteurs.[12] Cette loi comme son intitulé l'indique, a pour objet d'assurer la transparence des documents administratifs favorisant l'accès à ces derniers.

L'accès aux documents contenant des données à caractère personnel est soumis à de nombreuses conditions. En effet, la loi prévoit à l'article 6 paragraphe 1er qu'un tel document ne peut être communiqué qu'à la seule personne concernée par ses données personnelles. Encore est-il prévu, que lorsqu'un document ne contient pas uniquement des données personnelles de la personne ayant introduit la demande d'accès, mais également des données personnelles d'autres personnes, le document ne pourra être communiqué que lorsqu'il est possible ou bien « d'occulter ou de disjoindre » ces données à caractère personnel,[13] sous condition que cette opération n'occasionne pas de charge administrative excessive, ou si les personnes concernées donnent leur accord écrit ».[14]

Il s'avère donc que dès qu'un document contient des données personnelles, la législation sur la protection des données s'applique[15] étant donné qu'une communication de documents ne pourra être faite que si les données personnelles peuvent être supprimées ou si la personne concernée par les données en question a consenti par écrit à leur communication à un tiers.

Lorsqu'une demande de droit d'accès à des documents administratifs détenus par la CNPD est effectuée, celle-ci devra tenir compte des critères précédemment décris pour faire droit ou non à ladite requête.

La loi prévoit certes les modalités d'accès ainsi que celles de la communication des documents mais ce qui attire notre attention est la mise en place d'une Commission d'accès aux documents (ci-après désignée « CAD »), dont un représentant de la CNPD fait partie, veillant au respect du droit à la protection des données.[16] Lorsqu'une personne demandant l'accès aux documents se voit opposer un refus de communication, celle-ci peut saisir la CAD qui est une instance administrative indépendante et consultative.[17] Les avis de la CAD sont purement consultatifs, ne sont en aucun cas contraignants et ne peuvent pas faire l'objet d'un recours en justice.

12 Loi du 14.9.2018 relative à une administration transparente et ouverte. Voir également la lettre circulaire aux départements ministériels, administrations et services de l'Etat du 26 octobre 2018 par le Premier ministre d'Etat Xavier Bettel p. 2.

13 Loi du 14.9.2018 relative à une administration transparente et ouverte, art. 5(2)(3).

14 *Ibidem*.

15 Avis de la CNPD du 26.2.2016 – Projets de loi N° 6810 et 6811, p. 5.

16 Projet de loi N° 6810, Exposé des motifs, Commentaire des articles, ad art. 9, p. 9.

17 Loi du 14 septembre 2018 relative à une administration transparente et ouverte, art 10. Voir également, Lettre circulaire aux départements ministériels, administrations et services de l'Etat du 26 octobre 2018 par le Premier ministre d'Etat Xavier Bettel, p. 4.

f) Mise en œuvre de l'article 87 du RGPD

L'article 87 du RGPD permet aux Etats membres de préciser des conditions spécifiques du traitement du numéro d'identification national ou tout autre identifiant d'application générale, tout en stipulant que des « garanties appropriées pour les droits et libertés de la personne concernée » en vertu du RGPD doivent être en place. Les règles précisant les conditions spécifiques du traitement du numéro d'identification national sont d'ores et déjà prévues par la loi du 19 juin 2013 relative à l'identification des personnes physique. Ces règles n'ont donc pas été adoptées lors de l'entrée en application du RGPD, mais sont néanmoins importantes pour préciser les conditions du traitement du numéro d'identification national.

Le registre national des personnes physiques (ci-après désigné « RNPP ») contient des données personnelles, telles que le numéro d'identification national de chaque personne. Lors de l'élaboration de la loi du 19 juin 2013 relative à l'identification des personnes physique, il avait été envisagé de remplacer le numéro d'identification national actuel, composé de 13 chiffres faisant référence à certaines données personnelles de chaque individu,[18] par un numéro non-parlant dit « aléatoire » dans le but de renforcer la protection des données.[19] Ce projet a toutefois dû être abandonné après avis du Conseil d'État pour des raisons pratiques. La CNPD a cependant estimé qu'un numéro aléatoire serait « plus respectueux en matière de protection des données à caractère personnel ».[20] En effet, le lien du matricule aux données personnelles telles que la date de naissance est susceptible de créer un risque d'abus puisqu' une fois qu'on a connaissance de la date de naissance d'une personne, il ne reste plus qu'à se souvenir des derniers chiffres du matricule pour le recomposer.[21] Admettant que la mutation vers un numéro aléatoire comporte des coûts financiers et techniques, la CNPD s'est référée à l'exemple de la Suisse qui a opéré cette même mutation durant une période de transition de 1 ans et demi.[22]

Néanmoins, la loi du 19 juin 2013 relative à l'identification des personnes physiques vise à renforcer la protection des données à bien des égards. Premièrement, le matricule national comporte des chiffres de contrôle[23] ce qui permet d'éliminer des erreurs de saisie humaines ou par ordinateur. Deuxièmement, les finalités exactes des registres de personnes physiques sont précisées à l'article 4 de la loi.[24] Troisièmement, des règles concernant le

18 A savoir: la date de naissance et le sexe. Il peut être précisé que le numéro est impair pour les personnes du sexe masculin, pair pour les personnes du sexe féminin.

19 Projet de loi N° 6330 relative à l'identification des personnes physiques, Exposé des motifs, pp.18-19.

20 Avis de la CNPD du 16.1.2012 - Projet de loi N° 6330 relative à l'identification des personnes physiques, p. 3.

21 *Ibidem*, p. 4.

22 *Ibidem*.

23 Projet de loi N° 6330, Exposé des motifs, p. 21.

24 *Ibidem*.

contrôle de l'accès aux données sont adoptées.[25] Quatrièmement, le citoyen pourra savoir quelles administrations ont consulté ses données.[26] Cinquièmement, le citoyen disposera de plusieurs moyens pour communiquer et rectifier ses données et la communication des données aux tiers est régie par les dispositions du chapitre 3 de la loi. *In fine*, la cohérence et la standardisation des procédures entre les différents registres est assurée.

Autre gage non négligeable en ce qui concerne la protection des données par ladite loi est la mise en place d'une Commission du registre national.[27] A cet égard, l'article 7 précise que le ministre n'accorde l'accès au registre national qu'après consultation de la Commission du registre national. L'accès aux données n'est accordé par le ministre que si cela est en conformité avec les dispositions concernant le registre national et la protection des données mais également après avis de la Commission du registre national. Ladite Commission est composée de sept membres, dont un délégué de la CNPD, qui veille au respect de la protection des données, et analyse au cas par cas les demandes d'accès au RNPP.[28] La Commission doit analyser en particulier le bien-fondé des demandes d'accès qui devront être suffisamment motivées. Il revient également à la Commission de préciser l'étendue de l'accès aux données en limitant celui-ci à certaines données spécifiques contenues dans le RNPP.

g) Mise en œuvre de l'article 88 du RGPD

L'article 88 du RGPD donne la possibilité aux Etats membres de prévoir « par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail ». À ce titre, la loi du 1er août 2018 portant modification et organisation de la CNPD et du régime général sur la protection des données, modifie le Code du travail Luxembourgeois en ce qui concerne le traitement de données à caractère personnel à des fins de surveillance dans le cadre des relations de travail.[29] En effet, l'article L.261-1 du Code du travail se voit modifié. Le traitement de données à caractère personnel à des fins de surveillance des salariés au travail doit respecter les conditions de licéité énoncées à l'article 6, paragraphe 1er, lettres a) à f) du RGPD. Cet article encadre la surveillance au travail dans trois cas précis à savoir: « 1. Pour les besoins de sécurité et de santé des salariés, 2. Pour le contrôle de production ou des prestations

25 *Ibidem.*
26 *Ibidem.*
27 Loi du 19.6.2013 relative à l'identification des personnes physiques, art. 11.
28 Projet de loi N° 6330, Exposé des motifs, ad art. 7, p. 25.
29 Loi du 1.8.2018 portant organisation de la CNPD et du régime général sur la protection des données, art. 70.

du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact, ou 3. Dans le cadre d'une organisation de travail selon l'horaire mobile […] ».[30]

Il incombe à l'employeur d'informer la représentation du personnel et les salariés préalablement à la mise en place de la surveillance. Il doit fournir aux salariés une description détaillée des finalités du traitement de données personnelles prévu, la forme et la mise en œuvre de la surveillance, la durée et les critères de conservation des données ainsi qu' « un engagement formel de l'employeur de la non-utilisation des données collectées à une finalité autre ».[31]

Il peut également être mentionné que la délégation du personnel ou les salariés faisant l'objet d'une telle surveillance peuvent effectuer une demande d'avis préalable à la CNPD dans les quinze jours suivant l'information préalable de l'installation dudit dispositif, une telle demande ayant un effet suspensif.[32] La CNPD dispose d'un mois pour formuler son avis. Une telle disposition a fait l'objet de nombreuses critiques étant donné la cacophonie que celle-ci peut créer si elle est mise en œuvre sachant qu'elle peut être perçue comme étant une demande d'autorisation à la CNPD celle-ci n'ayant toutefois plus vocation à en émettre.[33]

Bien que l'obligation d'autorisation préalable délivrée par la CNPD ne soit plus nécessaire pour que l'employeur puisse prendre des mesures de surveillance envers ses salariés, l'article 30 du RGPD impose tout de même aux responsables de traitement l'obligation de tenir un registre des traitements de données à caractère personnel effectués.[34] De plus, tout employeur souhaitant surveiller ses employés reste tenu de respecter les principes de base du traitement licite et loyal des données à caractère personnel, en plus des conditions spécifiques posées par l'article L.261-1 du Code du Travail. Les salariés faisant l'objet d'une surveillance qu'ils estiment illicite, peuvent introduire une réclamation auprès de la CNPD sur base de l'article L.261-1(5) du Code du Travail. Le Code du Travail punit pénalement le traitement illicite de données dans le cadre de la surveillance au travail par une peine d'emprisonnement de 8 jours à un an et une amende de 251 à 125000 euros.[35]

h) Mise en œuvre de l'article 89 du RGPD

L'équilibre à trouver entre le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques d'une part et les

30 *Ibidem*.
31 Code du Travail, art. L.261-1(2).
32 *Ibidem*, L.261-1(4).
33 Avis du Conseil d'Etat du 30.03.2018 – Projet de loi N°7184 portant organisation de la CNPD et du régime général sur la protection des données, p. 39. Voir également l'avis complémentaire du Conseil d'Etat concernant ledit projet de loi et les avis de la CNPD.
34 Lignes directrices en matière de vidéosurveillance de la CNPD, p. 2.
35 Code du Travail, art. L.261-2.

libertés de la personne concernée par le traitement de ses données d'autre part est également délicat à trouver. Des garanties sont nécessaires afin de préserver lesdites libertés et permettre que le traitement en question soit adéquat, pertinent et limité à ce qui est nécessaire au regard des finalités pour lesquelles il est mis en œuvre.

Contrairement au RGPD qui prévoit le traitement à des fins archivistiques dans l'intérêt public, le législateur luxembourgeois a choisi de ne pas inclure le traitement à des fins archivistiques dans l'intérêt public au sein de la loi du 1er août 2018 portant organisation de la CNPD pour la protection des données et du régime général sur la protection des données.[36] Ladite loi se limite au traitement à des fins de recherches scientifiques ou historique, ou à des fins statistiques.[37] La loi prévoit des dérogations aux droits prévus aux articles 15, 16, 18 et 21 du RGPD dans la mesure où ces droits risquent de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques telles que les recherches scientifiques, historiques et statistiques.[38] Une dérogation est également prévue en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel dans la mesure où ce traitement est nécessaire à des fins archivistiques. Ledit traitement doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.[39] L'ensemble de ces dérogations doivent respecter les mesures appropriées listées à l'article 65 de la loi telles que: la désignation d'un délégué à la protection des données;[40] la réalisation d'une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ou encore l'anonymisation et la pseudonymisation de ces dernières.

L'archivage dans l'intérêt public quant à lui est prévu dans la loi du 17 août 2018 relative à l'archivage. Cette loi a plusieurs objectifs à savoir: assurer la gestion et la justification des droits des personnes physiques ou morales, publiques ou privées, mais aussi de garantir l'accès à la documentation d'intérêt historique, culturel, économique ou sociétal du Grand-Duché du Luxembourg.[41] Elle permet l'encadrement du versement des archives publiques ou aux archives nationales ainsi qu'une sélection et la destruction des archives publiques. La loi prévoit également des dispositions relatives à l'encadrement de la gestion et de la conservation des archives publiques, ainsi que leur protection.

36 L'archivage dans l'intérêt public fait l'objet d'une loi spécifique.

37 Loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données, Titre II, chapitre 2.

38 *Ibidem*, art. 63.

39 RGPD, art. 9(2)(j).

40 Loi du 1.8.2018 portant organisation de la CNPD et du régime général sur la protection des données, art. 65(1).

41 Loi du 17.8.2018 relative à l'archivage, art. 1.

Il ne peut pas être ignoré que les archives, qu'elles soient privées ou publiques, contiennent des données à caractère personnel auxquelles une personne concernée par celles-ci souhaite avoir accès. Ce droit d'accès doit s'effectuer conformément à l'article 15 du RGPD.[42] Des dérogations aux articles 16, 18, 20 et 21 sont néanmoins prévues. En effet, les personnes concernées dont les données à caractère personnel sont contenues dans les documents archivés ne peuvent pas exiger la rectification des données et la limitation de leur traitement, ou encore faire valoir leur droit d'opposition audit traitement.

i) Mise en œuvre de l'article 90 du RGPD

La loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données à l'article 67, révèle que le Luxembourg se dote de règles spécifiques afin d'encadrer les pouvoirs d'accès de la CNPD visés à l'article 58, paragraphe 1, points e) et f) du RGPD à l'égard des responsables du traitement ou des sous-traitants soumis à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes.[43] En effet, la loi prévoit des conditions d'accès spécifiques dans le cadre de l'accès auprès ou à l'égard d'un avocat, d'un notaire, d'un professionnel de l'audit.[44] Pour assurer la protection des obligations de secret professionnel des avocats, notaires et auditeurs quant aux données personnelles obtenues dans le cadre d'une activité couverte par leur secret professionnel,[45] l'article 67 renvoi aux lois qui régissent ces professions. Il s'agit en effet d'une généralisation du régime de protection du secret professionnel face aux perquisitions et saisies par les autorités répressives ou judiciaires, qui s'applique à travers l'article 67 de la loi également à la CNPD.

Question 2

Actuellement la Constitution luxembourgeoise n'établit aucune distinction entre les deux droits étant donné que seul le droit au respect de la vie privée est garanti à l'article 11(3) de la Constitution. La protection de la vie privée fait également l'objet d'une loi spécifique, celle du 11 août 1982 toujours applicable aujourd'hui. Dans l'ordre juridique national, le droit à la protection des données est considéré comme étant d'inspiration européenne,[46] un tel droit n'ayant pas existé en droit luxembourgeois avant sa création au niveau européen.

42 *Ibidem*, art. 19.
43 Conformément à l'article 90(1) RGPD.
44 Loi du 1.8.2018 portant organisation de la CNPD et du régime général sur la protection des données, art. 67.
45 *Ibidem*, art. 67(4).
46 J-L Schiltz et M. Spielmann, *opt. cit.* 2, p. 135.

La distinction entre le droit au respect de la vie privée et le droit à la protection des données effectué par la Charte a cependant inspiré le dernier projet de réforme de la Constitution. En effet, la création d'un droit à l'autodétermination informationnelle et à la protection des données à caractère personnel, indépendant du droit au respect de la vie privée, y est envisagé.[47] La proposition de révision se réfère à l'article 8 de la Charte pour justifier l'inclusion de ce nouveau droit dans la Constitution.[48] Le choix de faire explicitement mention d'un droit à l'autodétermination informationnelle indique l'interprétation sous-jacente du droit à la protection des données dans le droit national.[49] Pour éclaircir la notion d' « autodétermination informationnelle » la Commission des institutions et de la révision constitutionnelle se réfère à l'arrêt *Volkszählungsurteil* du *Bundesverfassungsgericht* de 1983, qui a consacré la valeur constitutionnelle de ce principe dans le droit allemand.[50] Le principe de l'autodétermination informationnelle, étant fondé sur les valeurs de dignité humaine et d'autonomie individuelle, est bien connu dans la littérature académique pour avoir un lien inexorable avec la protection des données. En revanche, il n'est pas clair quant aux conséquences qu'aura son ancrage au niveau constitutionnel.[51]

Bien que la proposition de révision constitutionnelle se réfère à l'article 8 de la Charte, le champ d'application conceptuel de la protection des données en tant que droit fondamental indépendant par rapport au respect de la vie privée fait l'objet de débats académiques éclaircis par la jurisprudence de la Cour de justice de l'Union européenne (ci-après désignée « CJUE »).[52] En se référant à l'article 8 de la Charte comme source d'inspiration pour l'inclusion d'un droit à l'autodétermination informationnelle dans la Constitution luxembourgeoise, il peut être présumé que son interprétation suive la jurisprudence de la CJUE en la matière. Toutefois, certains auteurs luxembourgeois avertissent que la notion d'autodétermination informationnelle repose sur une logique patrimoniale de droit de propriété individuelle, une interprétation qui serait à éviter.[53] Il est important pour cela que le législateur luxembourgeois se réfère également à la jurisprudence de la cour constitutionnelle allemande qui ancre le droit à la protection des

47 Rapport de la Commission des institutions et de la révision constitutionnelle du 6.6.2018 – Proposition de révision N° 6030 portant instauration d'une nouvelle constitution, Commentaire des articles, ad art. 31, Rapport que l'on retrouve à la page https://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2019)006-f. Toutes les pages Web ont été consultées pour la dernière fois le 1.2.2020.

48 *Ibidem*.

49 *Ibidem*.

50 *Ibidem*; BVerfGE 65, 1 para. 95: *„… Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"*.

51 J-L Schiltz, 'Coffre-fort ou désert de données?' (Paperjam.lu, 6.4.2015) <paperjam.lu/article/rendez-vous-coffre-fort-ou-desert-de-donnees>.

52 Rapport de la Commission des institutions et de la révision constitutionnelle du 6.6.2018 – Proposition de révision N° 6030 portant instauration d'une nouvelle constitution, Commentaire des articles, ad art. 31.

53 J-L Schiltz et M. Spielmann, *opt. cit.* 2, p. 136.

données dans les droits fondamentaux de dignité humaine et l'autonomie individuelle. En tout état de cause, le droit à l'autodétermination informationnelle envisagé par le législateur luxembourgeois ne serait pas un droit absolu, il pourra faire l'objet de limitations prévues par la loi.[54]

B Réception des dispositions de fond du RGPD dans l'ordre juridique national

Question 3

Dans un arrêt du tribunal d'arrondissement de Luxembourg du 22 octobre 2014, le principe de minimisation des données a été décrit comme exigeant que seulement «le strict minimum nécessaire de données soient insérées dans une base de données (cf. Loi de 2002, art 4) ».[55] Cet arrêt constitue cependant une exception, étant donné que les cours luxembourgeoises répètent de manière générale la formule prévue à l'article 4 de la loi de 2002 qui transposait mot par mot l'article 6 Directive 95/46, qu'un responsable de traitement doit assurer que « les données traitées le soient loyalement et licitement, et que notamment ces données soient collectées pour des finalités déterminées explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités ».

La CNPD plaide également en faveur du traitement loyal, pour la limitation des finalités et la minimisation des données. Elle oriente les responsables de traitement en ce sens lors des demandes d'informations et des réclamations qui lui sont adressées.

Question 4

Le « consentement », a sous l'empire de la loi du 2 août 2002 été interprété de façon très protectrice par le législateur luxembourgeois comme devant exprimer une « volonté expresse et non équivoque » pour pouvoir être valable.[56] Entre temps cette interprétation a été abandonnée.[57] Le RGPD, mettant l'accent sur le caractère «libre, spécifique, éclairé et univoque » du consentement, exige que le consommateur ait un véritable choix lorsqu'il donne son consentement au traitement de ses données personnelles.[58] Dans un contexte

54 Voir par ex. Affaire TA Lux, 2.7.2014, n° du rôle 1872/2014.
55 Affaire TA Lux, 22.10.2014, n° du rôle 2697/2014.
56 J-L Schiltz et M. Spielmann, *opt. cit.* 2, p. 137.
57 *Ibidem*.
58 Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (WP 259 rev. 01, 10.4.2018) p. 5. "*if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid*".

de services numériques, on pourrait s'interroger s'il existe véritablement un libre choix, lorsque les seules options sont d'accepter le traitement de ses données personnelles et ainsi pouvoir accéder aux services numériques, ou de refuser le traitement de ses données et d'être refusé l'accès aux services numériques.

L'article 7, paragraphe 4, du RGPD prévoit que lorsque le consentement est utilisé pour justifier un traitement de données personnelles, au moment de déterminer si le consentement est donné librement, il y a lieu de tenir compte de la question de savoir si l'exécution d'un contrat est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. De même, l'article 6, paragraphe 1, sous b), dispose que le traitement est licite lorsqu'il « est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie » (mise en italique par nos soins).

Question 5

Aucune décision n'a été prise quant à la validité du transfert de données personnelles comme « contrepartie » à la fourniture de contenus numériques, en droit luxembourgeois.

Il est cependant envisageable que le législateur luxembourgeois et les juridictions luxembourgeoises s'inspirent des droits des pays voisins en cette matière. À l'exemple de la Recommandation 2014/02 de la Commission des clauses abusives française, il pourrait être fait usage de l'article L.122-4 du code de la consommation luxembourgeois. Cet article prévoit que le fait de « décrire un produit comme étant «gratuit», «à titre gracieux», «sans frais» ou autres termes similaires si le consommateur doit payer quoi que ce soit d'autre que les coûts inévitables liés à la réponse à la pratique commerciale et au fait de prendre possession ou livraison de l'article » est à considérer comme une pratique commerciale trompeuse réputée déloyale en toutes circonstances.[59] En outre, la Commission des clauses abusives française a maintenu que les clauses de gratuité « laissent croire à l'utilisateur consommateur ou non-professionnel que le service est dépourvu de toute contrepartie de sa part, alors que, si toute contrepartie monétaire à sa charge est exclue, les données, informations et contenus qu'il dépose, consciemment ou non, à l'occasion de l'utilisation du réseau social, constituent une contrepartie qui s'analyse en une rémunération ou un prix, potentiellement valorisable par le professionnel […] que ces clauses sont de nature à créer un déséquilibre significatif entre les droits et obligations des parties au contrat au détriment du consommateur ou du non-professionnel en ce qu'elles lui laissent croire qu'il ne fournit aucune contrepartie, alors que celle-ci réside dans l'ensemble des traitements

59 Le texte de cette disposition est identique à l'article L.121-4(19) du Code de la consommation français.

de ses données à caractère personnel, des informations et des contenus déposés sur le réseau ».[60]

La protection du consommateur au Luxembourg étant en plein développement, de tels raisonnements peuvent voir le jour dans un futur proche.

Question 6

Le Luxembourg n'a pas légiféré pour écarter le droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé, y compris le profilage tel qu'autorisé par l'article 22, paragraphe 2, sous b) du RGPD.

Question 7

Il n'y a aucune application spécifique au droit luxembourgeois par rapport au droit à l'oubli.[61]

Question 8

Des dérogations au régime de protection des données prévu par le RGPD ont été adoptées au Luxembourg pour la mise en œuvre du traitement « aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire » à l'article 62 de la loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données. Par rapport à l'ancien article 9 de la loi du 2 août 2002 en la matière, il n'y a pas de grands changements à noter, hormis ceux reflétant la prise en compte de l'objectif d'harmonisation complète du RGPD. À cet égard, il y a lieu de mentionner que la référence à la loi modifiée de 2004 sur la liberté d'expression dans les médias a été supprimée.[62] Bien que l'exercice de la liberté d'expression dans les médias reste régi par la loi modifiée de 2004, cette dernière n'ajoute aucune dérogation supplémentaire au niveau de protection des données à caractère personnel assuré par le RGPD. L'article 62 a vocation à régir totalement la conciliation entre les deux droits fondamentaux concernés en droit luxembourgeois.

60 Recommandation N°14-02: Contrats de fourniture de services de réseaux sociaux' (Commission des clauses abusives, 7 Novembre 2014) <www.clauses-abusives.fr/recommandation/contrats-de-fourniture-de-services-de-reseaux-sociaux-nouveau/>.

61 J-L Schiltz et M. Spielmann, *opt. cit.* 2, p. 138.

62 Les dérogations spécifiques pour la protection de la liberté d'expression étaient précédées dans l'article 9 de la Loi du 2 août 2002 par la mention: « Sans préjudice des dispositions prévues dans la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias ».

En terme de contenu, il est intéressant de noter que ledit article a conservé l'ancienne formulation, plus restrictive de l'article 9 Directive 95/46, au lieu d'adopter la nouvelle formulation du RGPD qui ne mentionne plus aucun critère d'exclusivité. Dans beaucoup d'État membres cette formulation avait été interprétée dans le cadre de la Directive 95/46 comme imposant une condition d'exclusivité à des fins du traitement. Plus précisément, le traitement devait avoir pour seule fin l'expression journalistique, artistique ou littéraire pour entrer dans le champ d'application de la dérogation.[63] L'objet de l'article 62 est de prévoir une dérogation globale en faveur de l'exercice du droit à la liberté d'expression et d'information qui s'applique dès qu'un traitement de données relève des domaines journalistiques ou de l'expression universitaire, artistique ou littéraire. Il incombe au juge de vérifier si ces finalités sont respectées.[64]

La première dérogation spécifique au régime de protection des données prévue par l'article 62(1), prévoit que la prohibition de traitement de catégories particulières de données à caractère personnel ne s'applique pas,[65] de même que les limitations de traitement de données judiciaires aux condamnations pénales et infractions,[66] et ce, si le traitement des données remplit trois conditions alternatives:[67]

1. Il doit se rapporter à des données rendues manifestement publiques par la personne concernée, il doit s'agir d'une « manifestation de volonté claire et non équivoque » de la personne concernée.[68]
2. Il doit être en rapport direct avec la vie publique ou le caractère public de la personne concernée.[69]
3. Le traitement se rapporte à des données en rapport avec un fait de caractère public dans lequel la personne concernée est impliquée de façon volontaire.[70]

La deuxième dérogation prévue par l'article 62(2) est une dérogation au chapitre V du RGPD, ce qui implique que le mouvement transfrontalier des données vers des pays tiers ou à des organisations internationales qui ne peuvent pas assurer un niveau de protection adéquat est permis dans le cadre de traitement de données à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire.[71]

---

63 D. Erdos, 'From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection' (2015) 52 *CMLRev* p. 119, p. 140.
64 Projet de loi N° 7184, Exposé des Motifs, ad art. 56, p. 27.
65 Loi du 1.8.2018 portant organisation de la CNPD et du régime général sur la protection des données, art 62(1)(a).
66 *Ibidem*, art. 62(1)(b).
67 Affaire TA Lux, décision du 11.10.2007, n° du rôle 2656/2007.
68 Projet de loi N° 7184, Exposé des Motifs, ad art. 56, p. 27.
69 *Ibidem*.
70 *Ibidem*, p. 28.
71 *Ibidem*.

La troisième dérogation prévue par l'article 62(3) permet de déroger à l'obligation d'information lorsque celle-ci « compromettrait la collecte des données auprès de la personne concernée ».[72] Cette dérogation aurait le but d'assurer une liberté d'action aux journalistes, pour qu'ils ne soient pas contraints de divulguer le sujet de leurs travaux journalistiques ou leurs méthodes journalistiques à une personne concernée.[73]

La quatrième dérogation prévue par l'article 62(4) permet de déroger à l'obligation d'information de la personne concernée lorsque des données sont collectées auprès d'une personne autre que celle concernée par les données, dans quatre cas de figure:[74] (1) lorsque remplir cette obligation compromet de quelque manière que ce soit la collecte des données, (2) lorsque remplir cette obligation compromet une publication en projet, (3) lorsque cela compromet la mise à disposition du public des données et enfin, (4) lorsque remplir cette obligation fournirait des indications permettant d'identifier la source d'information journalistique.[75]

La dernière dérogation prévue par l'article 62(5) limite le droit d'accès de la personne concernée.[76] En ce qui concerne la source de l'information, le droit d'accès doit être mis en balance avec les intérêts du journaliste.[77] Le droit d'accès concernant la source journalistique est donc indirect, et ne pourra qu'être accordé par l'intermédiaire de la CNPD.[78] A cet égard, il peut être ajouté qu'en cas d'accès de la CNPD aux lieux de travail journalistiques, la présence du Président du Conseil de Presse est requise pour veiller au respect des obligations déontologiques des journalistes, en particulier la protection des sources.[79]

C Application interne de la législation en matière de protection des données

Question 9

La CNPD est notamment compétente en ce qui concerne la bonne application du régime général sur la protection des données ainsi que pour contrôler et vérifier le respect des

72 Loi du 1.8.2018 portant organisation de la CNPD et du régime général sur la protection des données, art. 62(3).
73 Projet de loi N° 7184, Exposé des Motifs, ad art. 56, p. 28.
74 *Ibidem*.
75 Loi du 1.8.2018 portant organisation de la CNPD et du régime général sur la protection des données, art. 62(4).
76 *Ibidem,* art. 62(5).
77 Projet de loi N° 7184, Exposé des Motifs, ad art. 56, p. 28.
78 *Ibidem*.
79 *Ibidem*.

dispositions de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.[80] En revanche, la CNPD n'est pas compétente pour contrôler les opérations de traitement de données à caractère personnel effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles. Cette mission revient à l'autorité de contrôle de la protection des données judiciaires.[81] Il s'agit dans un premier temps de faire état des changements structurels qu'a connu la CNPD occasionné par l'entrée en application du RGPD (1) pour ensuite effectuer le bilan de la mise en œuvre du RGPD par la CNPD (2).

1) Les changements structurels connus par la CNPD

L'entrée en application du RGPD et son application directe en droit luxembourgeois à travers la loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données, ont eu pour effet de créer de nouvelles missions de la CNPD ou de renforcer celles existantes.

A l'aube de l'ère digitale et au lendemain de l'entrée en application du paquet « protection des données », la CNPD a dû se préparer à contrôler, auditer, sanctionner, répondre aux préoccupations grandissantes du public en matière de protection des données, à former et à sensibiliser les acteurs concernés afin de permettre une exploitation encadrée des données à caractère personnel des individus. Elle se doit également d'assoir de son autorité à l'échelle européenne au sein du CEPD.

Cette conjoncture entraîne des besoins de personnel conséquent. C'est la raison pour laquelle, en mars 2015, la CNPD a élaboré un « Concept de développement stratégique pour la période 2015-2019 » validé par le Gouvernement. Ce dernier a fait l'objet de nombreuses révisions afin de correspondre davantage aux changements occasionnés par le RGPD. Emane des dites révisions un besoin prévisionnel d'un effectif s'élevant à 62 postes à plein temps afin de permettre à la CNPD d'assurer son bon fonctionnement, de répondre à ses missions et de pouvoir respecter les délais imposés par le nouveau système.

Les effectifs de la CNPD comprennent des fonctionnaires et employés de catégories différentes.

Au début de l'année 2019, l'effectif de la CNPD s'élevait à 39 personnes et ce nombre devrait s'élargir à 48 d'ici la fin de cette même année.

Mais cet apport en effectif ne s'arrête pas là. La CNPD a toujours et encore besoin de ressources. En effet, pour la période 2020-2023, 14 personnes supplémentaires à savoir 12 agents de la carrière A1, appartenant au sous-groupe de traitement administratif ou

80 Loi du 1.8.2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, art. 39.

81 *Ibidem*, arts 40 sqq.

scientifique et technique, 1 agent de la carrière A2, appartenant au sous-groupe de traitement administratif et une personne de support administratif de la carrière B1 et toutes à plein temps pourraient venir rejoindre les équipes de la CNPD.

2) Le bilan d'activité de la CNPD favorisant la mise en œuvre du RGPD à l'échelle nationale[82]

En 2018, la CNPD a été plus fortement sollicitée que les autres années. Cette sollicitation émane à la fois de la nouvelle approche dite de responsabilisation émanant du RGPD et de la prise de conscience des enjeux de protection des données par les professionnels et les particuliers.

A titre d'exemples, la CNPD a reçu 1.112 demandes de renseignement par écrit en 2018, soit plus que le double qu'en 2017 où elle en avait reçu 528. Ce nombre élevé s'explique par l'effet médiatique du RGPD et des acteurs de plus en plus sensibilisés.

De nombreuses questions ont porté sur la mise en conformité à la nouvelle législation. D'autres demandes récurrentes concernaient notamment la vidéosurveillance (du domicile privé et sur le lieu de travail), le délégué à la protection des données ou encore le droit d'accès et les autres droits des personnes concernées (droit à l'effacement, droit d'opposition, droit de rectification, etc.).

La CNPD a par ailleurs, participé au processus législatif avec 27 avis (soit 5 de plus qu'en 2017) sur des projets de loi ou mesures règlementaires en lien avec la protection des données.

D'autre part, le nombre de réclamations traitées est jusqu'à présent le plus important de toute l'histoire de la CNPD.

Le nombre de réclamations de personnes qui ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits a plus que doublé par rapport à l'année précédente, de 200 en 2017 à 450 en 2018. Le RGPD a eu un impact important: lors des 5 premiers mois de l'année, la CNPD a reçu en moyenne 18 plaintes par mois, tandis que pour les 7 mois qui ont suivi, elle en a reçu 51 par mois.

En termes de sensibilisation, la CNPD a été on ne peut plus active. En effet, à l'occasion de l'entrée en application du RGPD, la CNPD a lancé sa campagne de sensibilisation « Vos données? Vos droits! ». Du 25 mai au 11 juin 2018, l'autorité de protection des données a organisé plusieurs événements, a distribué 12,000 brochures et gadgets dans de nombreux endroits stratégiques du Grand-Duché du Luxembourg et est intervenue dans les médias.

Le 4 juin 2018, la CNPD a réuni de prestigieux orateurs afin de célébrer 4 décennies de protection des données. Le premier Ministre, Monsieur Xavier Bettel, la Commissaire européenne à la justice, aux consommateurs et à l'égalité des genres, Madame Vera Jourova,

82 Pour plus de détails à cet égard, voir le Rapport annuel 2018 de la CNPD, à la page https://cnpd.public.lu/dam-assets/fr/publications/rapports/cnpd/rapport-annuel-%2B-annexes-2018-CNPD-BD.pdf.

et la présidente du Comité Européen de la Protection des Données, Madame Andrea Jelinek, y sont notamment intervenus.

La CNPD a également pris de nombreuses mesures de sensibilisation et de guidance en 2018.

Il y a également lieu de préciser que la CNPD a renforcé sa méthodologie d'enquête en ce qui concerne les audits et les contrôles sur place. En effet, La CNPD a adapté sa stratégie et mis en place des enquêtes dites « proactives ». Ces enquêtes sont effectuées sous la forme d'audits thématiques portant sur les nouvelles obligations du RGPD. En termes de chiffres, 12 enquêtes sur place ont eu lieu en 2018 dans les domaines de la vidéosurveillance, de la géolocalisation, de la publicité et du marketing.

En termes de violations de données, 172 violations de données ont été déclarées à la CNPD en 2018. La principale cause de violation de données à caractère personnel reste l'erreur humaine.

Il ressort de la présente réponse que la CNPD est en perpétuel mouvement afin de répondre tant au développement de l'ère digitale qu'aux obligations dictées par le RGPD. L'encadrement de l'exploitation des données à caractère personnel afin que celle-ci soit en accord avec les valeurs de l'Union européenne et les droits fondamentaux est au cœur des préoccupations de la CNPD.

Question 10

Il a été précédemment fait mention de l'important nombre des réclamations occasionné par une prise de conscience de l'importance des droits au respect de la vie privée et du droit à la protection des données à caractère personnel suite à l'entrée en application du RGPD. Avec un nombre de 450 réclamations adressées à la CNPD en 2018, une adaptation en termes de gestion de ces dernières est incontournable. Ladite adaptation s'est concrétisée à travers l'augmentation de l'effectif du département des réclamations permettant ainsi de traiter l'ensemble de ces dernières. Toutefois, un ordre de priorité peut être donné en fonction de la gravité ou du caractère urgent de la réclamation. Il peut également être précisé que dans la mesure du possible, le traitement des réclamations s'effectue à l'amiable.

La loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données ne prévoit pas de contraintes légales quant à la gestion des réclamations.

Question 11

A l'heure où le rapport est écrit, la CNPD n'a pas fait usage des nouveaux mécanismes introduits par le RGPD permettant aux autorités de contrôle de sanctionner. Par

conséquent, aucune sanction relative aux règles sur la protection des données n'a pour le moment été prononcée.

Question 12

La responsabilité civile est consacrée en droit luxembourgeois à l'article 1382 du code civil qui dispose que « tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer ». Cet article formulé en des termes généraux permet de s'adapter à son temps, aux nouvelles situations.[83] Il a favorisé la création d'un droit essentiellement jurisprudentiel.

En ce qui concerne plus particulièrement la notion de préjudice moral, il est important de préciser qu'elle n'est pas juridiquement définie. Néanmoins, le dommage moral peut être perçu comme un préjudice « […] que subit l'individu dans sa personne en dehors de toute blessure physique, et qui se traduit par une atteinte à des liens d'affection, à son nom, à sa réputation, à l'honneur, à l'image, à la vie privée ».[84]

L'allocation d'intérêts est permise à travers une interprétation souple du dommage, c'est notamment le cas lors du préjudice portant atteinte aux droits de la personnalité tel que celui à la vie privée. En effet, il s'avère que le préjudice moral engendré par une atteinte aux droits de la personnalité est plus souvent théorique que réellement constitué ou démontré.[85] La jurisprudence luxembourgeoise révèle qu'en matière d'atteinte à la personnalité, la démonstration du préjudice n'est généralement pas très rigoureusement contrôlée dès lors que la faute, telle que l'atteinte illicite à la vie privée est établie.[86]

L'atteinte illicite à la protection des données à caractère personnel peut également être considérée comme une atteinte aux droits de la personnalité. Un préjudice moral peut parfaitement émaner d'une telle atteinte si celle-ci est établie. Pour l'heure, il n'existe pas encore de jurisprudence relative à une telle situation. Néanmoins, il peut être précisé que le RGPD prévoit un droit au recours juridictionnel effectif contre une autorité de contrôle[87] et contre un responsable du traitement ou un sous-traitant[88] en ce qui concerne tout traitement présumé illicite de ses données personnelles. Cela signifie que, lorsque la CNPD n'établit pas qu'il y a eu une atteinte illicite au droit à la protection des données à caractère personnel au moment où elle est saisie d'une réclamation, la personne concernée peut

83 G. Ravarani, *La responsabilité civile des personnes privées et publiques* (3ème Ed, Pasicrisie luxembourgeoise 2014), p. 22.

84 *Ibidem*, p. 1132.

85 *Ibidem*, p. 1134. L'auteur précise notamment qu'en ce qui concerne la vie privée, les droits de la personnalité sont protégés par la loi du 11.8.1982 concernant la protection de la vie privée.

86 *Ibidem*, l'auteur fait notamment référence au jugement de la Cour d'appel du 15.6.2000.

87 Voir également la Loi du 1.8.2018 portant organisation de la CNPD, arts 55 et 78.

88 *Ibidem*, art. 79.

contester la décision de la CNPD. Par conséquent, la décision de la CNPD résultant de l'introduction de la réclamation ne conditionne pas l'appréciation du préjudice moral à *posteriori*.

Question 13

A l'heure où l'économie digitale bouleverse le droit de la consommation et crée des attentes du côté consommateurs, des autorités ainsi que des régulateurs en termes de la protection de leurs données notamment en matière commerciale, le RGPD donne la possibilité aux Etats-membres de légiférer afin que tout organisme puisse avoir le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente.[89]

Le Luxembourg n'a pour l'instant pas introduit une telle possibilité en droit national. L'inexistence du droit d'introduire une réclamation à la CNPD émanant de l'Association pour la Protection des données au Luxembourg ou encore de l'Union Luxembourgeoise des Consommateurs n'est donc pour l'instant pas possible[90]. La ministre de la Protection des Consommateurs, Madame Paulette Lenert a récemment rappelé le besoin d'introduire l'action collective en justice en droit luxembourgeois. En matière du droit à la protection des données à caractère personnel, un tel besoin s'est notamment fait ressentir lors de l'affaire *Cambridge Analytica*. Si l'introduction d'une telle action fait l'objet de nombreux débats,[91] elle devrait se concrétiser à l'avenir.[92] En effet, le Luxembourg devrait suivre les initiatives prises à l'échelle de l'Union européenne[93] afin de moderniser le droit à la consommation et renforcer la protection juridique au sein de l'Union européenne.[94]

Question 14

Ayant conscience de la valeur économique et de la valeur relative à la dignité humaine des données à caractère personnel, il y a des interactions ponctuelles entre la CNPD et les régulateurs tels que l'Institut Luxembourgeois de Régulation mais aussi avec l'Union

89 RGPD, art. 80(2).
90 De Konsument 04/2019, pp. 8-9.
91 Menétrey S., Recours collectif- Défis pour le Luxembourg, Table ronde du 6.6.2018, p. 1.
92 De Konsument 03/2017, pp. 6-7.
93 Recommandation de la Commission du 11.6.2013 relative à des principes communs applicables aux mécanismes de recours collectif en cessation et en réparation dans les Etats membres en cas de violation des droits conférés par le droit de l'Union européenne.
94 *Ibidem*, voir également, la proposition de Directive du 11.4.2018 relative aux actions représentatives dans le domaine de la protection d'intérêts collectifs des consommateurs.

Luxembourgeoise des consommateurs lors de réclamations relatives au traitement de données par les services de communications électroniques.[95]

En outre, la coopération entre les différentes autorités est essentielle. Compte tenu de l'absence de possibilité d'action collective en justice comme précédemment mentionné ou encore de la récente création du ministère de la protection des consommateurs,[96] la collaboration entre la CNPD et les autorités compétentes n'est qu'à ses débuts et vise à se renforcer. De surcroît, la CNPD fait partie du réseau *Digital Clearinghouse*[97] dont le but est de créer une plateforme favorisant la coopération et le partage d'expérience entre les autorités, les décideurs ainsi que des chercheurs. Prendre part à un tel réseau permet de traiter des sujets liés à la concurrence, à la protection des données à caractère personnel et la protection des consommateurs.

D Traitement de données pour des motifs de sécurité nationale

Question 15

La notion de « sécurité nationale » est définie en droit luxembourgeois par l'article 2 point 13, de la loi du 27 juin 2018 relative au contrôle des exportations qui définit la sécurité nationale pour les besoins de ladite loi comme « l'indépendance et la souveraineté de l'État, la sécurité et le fonctionnement des institutions, les droits fondamentaux et les libertés publiques, la sécurité des personnes et des biens, le potentiel scientifique et technique ou les intérêts économiques du Grand-Duché de Luxembourg». Il est évident que la sécurité nationale n'est pas exercée uniquement lors du contrôle des exportations, elle va bien au-delà de ce domaine et concerne bons nombre d'acteurs tels que le Service de renseignement de l'Etat[98] et la Police grand-ducale. A ce titre, il peut être noté que le législateur luxembourgeois a fait le choix d'étendre le champ d'application de la loi luxembourgeoise de transposition de la directive 2016/680, à savoir, la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, aux traitements de données personnelles effectués pour des motifs de « sécurité nationale ».

95 En 2018, le nombre de demandes de médiation relatives au domaine des services de communications électroniques était le plus important (117) par rapport à celles introduites dans le domaine de l'électricité (8) et dans le domaine des services postaux (4). In rapport d'activité annuel du service « Médiation » 2018, voy. web.ilr.lu/mediation/FR/Mediation/Informations-utiles/Publications/Pages/default.aspx/.

96 Depuis le 9.12.2018, Arrêté grand-ducal du 5.12.2018 portant constitution des Ministères, art. 1, point 19.

97 Ce projet est une initiative du contrôleur européen de la protection des données. Voy. www.digitalclearinghouse.org/.

98 Loi modifiée du 5.7.2016 portant réorganisation du Service de renseignement de l'État, art. 3.

Le législateur luxembourgeois a donc fait le choix d'étendre le champ d'application de la loi du 1er août 2018 précitée à la sécurité nationale.

A ce jour, la loi luxembourgeoise n'a pas effectué de modifications suite aux affaires jointes *Tele 2 et Watson*. A titre d'exemple, l'article 5 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques dispose que « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services ou opérateur qui traite des données relatives au trafic est tenu de conserver ces données pendant une période de douze mois ».[99] Ce même article détaille le traitement de ces données de trafic à des fins pénales dont la liste apparaît conséquente.[100] La loi prévoit également le traitement de données de localisation autres que les données relatives au trafic à des fins pénales.

Par conséquent la loi luxembourgeoise ne prévoit pas pour le moment un traitement ciblé des données de trafic à des fins pénales. Des garanties[101] et des voies de recours[102] pour les personnes concernées sont néanmoins prévues par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Un projet de loi est également en cours d'élaboration de rendre la loi luxembourgeoise conforme au droit de l'Union européenne et à la jurisprudence de la CJUE.[103]

99 Loi modifiée du 30.5.2005 concernant la protection de la vie privée dans le secteur des communications électroniques, art. 5(1).

100 Règlement grand-ducal du 24.7.2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communication électroniques ou de réseaux de communications publics.

101 Loi du 1.8.2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, chapitre 3.

102 *Ibidem*, chapitre 7.

103 Projet de loi N°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30.5.2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Malta

Mireille M. Caruana[*]

A Setting the Scene

Question 1

The main national legal instrument introduced to implement Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR")[1] in Malta is the Data Protection Act 2018 (hereinafter "DPA"),[2] which repealed and replaced the Data Protection Act of 2001[3] which was the legislation that transposed Directive 95/46/EC.[4] Subsidiary legislation has also been passed under the main Act, for example the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations,[5] transposing Directive (EU) 2016/680.[6]

Restrictions

Regulations enacted under article 5 DPA state that any restrictions to the rights of the data subject referred to in article 23 GDPR only apply where such restrictions are a necessary

* Lecturer, Department of Media, Communications and Technology Law, Faculty of Laws, University of Malta. The author would like to thank Ian Deguara and David Cauchi at the Office of the Information and Data Protection Commissioner, as well as David E. Zammit and Antoine Camilleri for their input when writing this report. The usual disclaimer applies.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Chapter 586, Laws of Malta.

3 Chapter 440, Laws of Malta.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

5 S.L. 586.08.

6 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119/89.

measure required for the interests listed therein,[7] and provide for broadly formulated safeguards including retention periods.[8]

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 9 GDPR provides that processing of defined 'special categories of personal data' is allowed if such processing 'is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) GDPR based on Union or Member State law (…).'[9] The DPA provides that the controller must consult with, and obtain prior authorisation from, the Information and Data Protection Commissioner (hereinafter "IDPC")

> where the controller intends to process in the public interest:
> a. genetic data, biometric data or data concerning health for statistical or research purposes; or
> b. special categories of data in relation to the management of social care services and systems, including for the purposes of quality control, management information and the general national supervision and monitoring of such services and systems:
>
> Provided that, where genetic data, biometric data or data concerning health are required to be processed for research purposes, the Commissioner shall consult a research ethics committee or of an institution recognised by the Commissioner for the purposes of this article.[10]

The research ethics committee consulted by the IDPC is the University Research Ethics Committee's sub-committee on data protection (hereinafter "UREC-DP").[11] It is doubtful that this national law satisfies the description provided by the GDPR (that the law must 'be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject'). In effect, the requirement of a law is replaced by a requirement of prior authorisation; and arguably it is envisaged that the Commissioner, having consulted UREC-DP, will ensure that there is proportionality, respect of the essence of the right to data protection, etc. prior to granting authorisation.

---

7 S.L. 586.09 Restriction of the Data Protection (Obligations and Rights) Regulations, regulation 4(a)-(i).
8 Ibid, regulations 5-7.
9 Art. 9(2)(j) GDPR.
10 Art. 7 DPA.
11 Webpage: www.um.edu.mt/urec. All webpages referred to were visited on 31 January 2020.

Article 6 DPA provides that (subject to appropriate safeguards for the rights and freedoms of the data subject) controllers and processors may derogate from the provisions of the GDPR relating to the right of access,[12] the right to rectification,[13] the right to restriction of processing[14] and the right to object[15] to the processing of personal data for scientific or historical research purposes or official statistics.[16] Controllers and processors may also derogate from the aforementioned provisions and additionally from the GDPR provisions relating to the notification obligation regarding the rectification or erasure of personal data or restriction of processing,[17] and the right to data portability[18] for the processing of personal data for archiving purposes in the public interest. In both instances such derogations are allowed 'in so far as the exercise of the rights set out in those Articles: (a) is likely to render impossible or seriously impair the achievement of those purposes; and (b) the data controller reasonably believes that such derogations are necessary for the fulfilment of those purposes.' Where such data processing serves at the same time another purpose, the derogations apply only to processing for the purposes referred to in the said article. This national provision is an implementation of the exemptions allowed in article 89(2) and (3) GDPR, transposed in terms which closely follow those of the GDPR.

Processing of the national identification number

Article 8 DPA provides that an identity document[19] may only be processed when such processing is 'clearly justified having regard to the purpose of the processing and – (a) the importance of a secure identification; or (b) any other valid reason as may be provided by law: Provided that the national identity number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to the Regulation.' This is clearly an implementing provision of article 87 GDPR. The terminology of the GDPR is closely followed and the local implementation does not add anything of substance thereto. In practice, in Malta it is not uncommon for

12 Art. 15 GDPR.
13 Art. 16 GDPR.
14 Art. 18 GDPR.
15 Art. 21 GDPR.
16 'Official statistics' is a term defined in the legislation as 'information collected, analysed and produced for the benefit of the society to characterize collective phenomena in a considered population and produced by the National Statistics Office as provided for by law, or by other national authorities as designated by Eurostat following recommendation by the National Statistics Office.'
17 Art. 19 GDPR.
18 Art. 20 GDPR.
19 'Identity document' is defined as a legally valid identity document as provided in the Identity Card and Other Identity Documents Act (chapter 258 of the Laws of Malta).

national identity numbers to be collected and processed and such is often done without regard to strict necessity requirements.[20]

Processing and freedom of expression and information

Article 9(1) DPA provides that 'personal data processed for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with the provisions of the GDPR specified in sub-article (2) where, having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with any of the provisions as specified in sub-article (2) would be incompatible with such processing purposes: Provided that when reconciling the right to the protection of personal data with the right to freedom of expression and information, the controller shall ensure that the processing is proportionate, necessary and justified for reasons of substantial public interest.'

Article 9(2) DPA is an implementation of article 85(2) GDPR. This includes exemptions from chapters II (principles relating to processing) (but no exemption from article 9 GDPR, processing of special categories of personal data), III (rights of the data subject), IV (controller and processor) and VII (co-operation and consistency). Specific articles of the GDPR are cited in the national law, omitting those articles or sub-articles where exemptions would be unwarranted or inapplicable to the data processing envisaged; for e.g. it is not unreasonable to exclude the right to rectification provided for in article 16 GDPR from the list of articles compliance with which may be exempted in the situations envisaged by article 85 GDPR and article 9 DPA. The national legislation of Malta does not provide for exemptions from GDPR chapters V (transfers of personal data to third countries or international organisations), VI (independent supervisory authorities) and IX (specific data processing situations). This assessment of the exemptions 'necessary to reconcile the right to the protection of personal data with the freedom of expression and information' (article 85(2) GDPR) does not appear to be problematic.

Article 9(2) DPA excludes article 9 GDPR from the list of articles from which exemption is granted where personal data are processed 'for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression' where compliance with any of the said provisions (specified in sub-article (2)) would be incompatible with such processing purposes. Is this potentially problematic, e.g. reporting that a politician who campaigns for criminalisation of homosexuality turns out to be gay? Article 9(2)(g) GDPR could provide the appropriate legal base, but then that should be 'on the basis of Union

20 This practice is generally uncontroversial in Malta and as a result documentary evidence to support this claim is not available.

or Member State law', where reference would, in this author's opinion, need to be made to the Media and Defamation Act.[21]

Transborder Data Transfers

Article 10 DPA provides that in the absence of an adequacy decision pursuant to article 45(3) GDPR, the Minister responsible for data protection may, following consultation with the IDPC, by regulations set limits to the transfer of specific categories of personal data to a third country or an international organisation for important reasons of public interest. This appears to be an implementation of article 49(5) GDPR. Rather than actually implement the option, the DPA allows for such possible future implementation by subsidiary legislation.

The Information and Data Protection Commissioner (IDPC)

The office of the Information and Data Protection Commissioner (hereinafter "IDPC") is set up under article 11 DPA. In implementation of article 58(1)(f) GDPR, the national law provides that in the exercise of the investigative powers pursuant to article 58 GDPR, or any other law, the Commissioner may request the assistance of the executive police in order to enter and search any premises.[22] The national law further provides that in the event of joint operations with supervisory authorities of one or more other Member States, the IDPC may, where appropriate, 'confer powers, including investigative powers, on the seconding supervisory authority's members or staff: Provided that such powers are exercised under the guidance and in the presence of the IDPC.'[23] This provision appears to be implementing article 62(3) GDPR.

Question 2

Unlike the EU Charter of Fundamental Rights (hereinafter "Charter"), our national legal order does not distinguish between the right to respect for private life and the right to data protection.

Article 32[24] of the Constitution of Malta provides:

21 Media and Defamation Act 2018, chapter 579, Laws of Malta.

22 Art. 16(1) DPA.

23 Art. 16(2) DPA. Under national law, 'Commissioner' means the Information and Data Protection Commissioner appointed under article 11 and includes any officer or employee of the Commissioner authorised by him in that behalf.

24 Which, while entrenched, is at the same time declared by art. 46 to be non-justiciable, unlike the rest of the provisions in Chapter IV of the Constitution, which are declared to be justiciable.

> Whereas every person in Malta is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex, sexual orientation or gender identity, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely –
>
> a. life, liberty, security of the person, the enjoyment of property and the protection of the law;
> b. freedom of conscience, of expression and of peaceful assembly and association; and
> c. *respect for his private and family life*,
>
> the subsequent provisions of this Chapter shall have effect for the purpose of affording protection to the aforesaid rights and freedoms, subject to such limitations of that protection as are contained in those provisions being limitations designed to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest.[25]

This pre-ambular set of limitations is reflected in specific provisions legitimising derogation in the case of each right (except for protection from inhuman or degrading treatment), such as by a provision of law which is 'reasonably required in the interest of public safety, public order, public morality or decency, public health or the protection of the rights and freedoms of others'. Several provisions speak both of 'reasonably required' and 'reasonably justifiable in a democratic society'. The standard is substantially similar to that of the European Convention on the Protection of Human Rights and Fundamental Freedoms of 1950 (hereinafter "ECHR").

Article 38 of the Constitution of Malta refers in a very limited fashion to the fundamental right of bodily and spatial privacy ('no person shall be subjected to the search of his person or his property or the entry by others on his premises') without any trace of a reference to modern concerns regarding for example informational and communications privacy.

The protection of fundamental rights in Malta is enhanced by the ECHR, as incorporated into Maltese law by virtue of the European Convention Act,[26] which extended the same right of action to the new rights derived therefrom.[27]

There is no tangible evidence regarding the manner in which the Charter right to data protection may have influenced the interpretation of national law.

---

25 Emphasis added.
26 Chapter 319, Laws of Malta.
27 Art. 3, European Convention Act.

Nevertheless, article 8 of the Charter was quoted in the judgment of Dr Jeffrey Pullicino Orlando v the Information and Data Protection Commissioner.[28] This case concerned the sharing on the blog 'Running Commentary: Daphne Caruana Galizia's Notebook', of articles including pictures of the claimant, a public figure (formerly a member of the national Parliament, later the Chairman on the Malta Council for Science and Technology), in public but not while exercising his official functions, and disclosing elements of his private life, for e.g. at a restaurant or at the airport with his partner. The right to privacy, as well as the right to data protection, and the rights relating to freedom of expression and journalistic freedoms were all mentioned in this judgment. The Hon. Mr Justice Anthony Ellul, the judge in the case, was not concerned with distinguishing the right to privacy from the right to data protection, but he did note that the definition of 'personal data' in terms of article 2 of the DPA 2001 is a wide one, and therefore also includes information regarding the geographical position of a person at a particular time.

Referring to the *Lindqvist* case,[29] the judge explicitly considered the collection of this data and its uploading and sharing on Daphne Caruana Galizia's blog to be an instance of 'processing' of personal data. The fact that that information concerned matters that happened in public did not change the fact that processing of personal data had occurred. Quoting article 8 of the Charter, the judge proceeded to consider the appropriate balance of the fundamental rights to privacy and to freedom of expression.[30] Case-law of the European Court of Human Rights (hereinafter "ECtHR") was referred to and quoted.[31] Overturning an earlier decision of the IDPC, the judge ruled that although the claimant was photographed in public places, nevertheless the publication of that information on-line amounted to processing of personal data, and concluded that the claimant's rights had in fact been breached as a public interest in sharing that private information had not been made out.

28 Court of Appeal (Civil, Inferior), 30 April 2019.

29 Judgment of 6 November 2003 in Case C-101/2001, *Criminal proceedings against Bodil Lindqvist*, ECLI:EU:C:2003:596.

30 Court of Appeal (Civil, Inferior), 30 April 2019, at para. 14.

31 In particular, *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, ECHR 607 (2017) App. No. 931/13.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

In Maltapost p.l.c. vs Information and Data Protection Commissioner,[32] the Maltese Court of Appeal (Inferior Competence) annulled a decision of the Information and Data Protection Appeals Tribunal[33] and confirmed the original decision of the IDPC. Referring to the 'European Document Retention Guide 2013',[34] as well as to the 2010 Guidelines published by the Office of the EDPS,[35] the Court ruled that the IDPC was right to establish that CCTV footage should, as a general rule, be deleted after a maximum period of seven (7) days. It also agreed that the IDPC was correct to establish a maximum retention period of twenty (20) days for a high-risk area in view of the special circumstances and the nature of work carried out in that area. The judgement interprets the former national Data Protection Act, which transposed Directive 95/46 and has now been repealed and replaced by the GDPR and the DPA.

Question 4

To the best of this author's knowledge, there have been no such interpretations handed down by our national courts.

Question 5

To the best of this author's knowledge there is to date no evidence of any debate or decision at national level regarding the validity of personal data as 'counter-performance' for the provision of digital content. However this author submits that personal data could be considered as a 'lawful consideration' in terms of s.966(d) of the Maltese Civil Code,[36] and thus the validity of the contract would be upheld by a court of law.[37]

32 Court of Appeal (Inferior competence), Appeal number 26/2017, 5 October 2018.

33 Set up under art. 24 DPA.

34 See: www.project-consult.de/files/Iron%20Mountain%20Guide%202013%20European%20Retention%20Periods.pdf.

35 The EDPS Video-Surveillance Guidelines, Brussels, 17 March 2010: edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf.

36 Civil Code, chapter 16 of the Laws of Malta.

37 Civil Code s.987: 'An obligation without a consideration, or founded on a false or an unlawful consideration, shall have no effect'; Civil Code s.988. 'The agreement shall, nevertheless, be valid, if it is made to appear

Question 6

No; Malta has not introduced legislative measures to ensure the right not to be subject to automated decision-making, including profiling, does not apply in certain situations, pursuant to article 22(2)(b) GDPR.

Question 7

In Malta there has been considerable controversy surrounding the decision to allow the request for erasure of certain on-line (criminal) court judgments from the public record.[38] The request was made to the court registrar who is the Courts' data controller. The Malta IT Law Association (hereinafter "MITLA") expressed concern, stating that: 'The application of the right to be forgotten with respect to public records needs transparent, justifiable rules.'[39]

It was reported in the local press that the Justice Minister had reported in Parliament that a total of 176 requests for court judgements to be removed from the public domain had been filed; of those, 112 judgements were made anonymous, meaning that the personal details of individuals were removed; 41 requests were rejected; one request was invalid; and another 22 requests were under consideration. One request was made in 2014; 21 requests in 2017; 121 requests in 2018; and 33 requests in 2019.[40]

Question 8

Malta has not introduced a law pursuant to article 85(2) GDPR beyond that described in the response to Question 1 above, i.e. article 9 DPA.

---

that such agreement was founded on sufficient consideration, even though such consideration was not stated.'

38 See for example Times of Malta, Court judgment can now 'be forgotten' – former minister expresses disbelief at the decision, 9 March 2018, www.timesofmalta.com/articles/view/20180309/local/law-students-request-to-be-removed-from-database-accepted.672714?utm_source=tom&utm_campaign=top5&utm_medium=widget; Times of Malta, 22 judgments removed from the court's online database, 12 April 2018, www.timesofmalta.com/articles/view/20180412/local/22-judgments-removed-from-courts-online-database.676092.

39 Statement by MITLA, 16 March 2018, accessed at www.mitla.org.mt/wp-content/uploads/2018/03/MITLA-Statement-16032018-MITLA-Right-to-be-Forgotten.pdf.

40 The Malta Independent, Court judgments removed from internet: Right to be forgotten must be respected – Bonnici, 17 May 2019, www.independent.com.mt/articles/2019-05-17/local-news/Court-judgments-removed-from-internet-Right-to-be-forgotten-must-be-respected-Bonnici-6736208252. Note: In Malta the decisions of the Office of the IDPC are not made publicly available for consultation.

C Domestic Enforcement of Data Protection Law

Question 9

The relevant public authority is the IDPC.[41]

The Commissioner is appointed by the Prime Minister after consultation with the Leader of the Opposition, to perform the duties of supervisory authority for the purposes of chapter VI of the GDPR.[42] The IDPC is responsible for monitoring and enforcing the application of the provisions of the DPA and the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing of personal data and to facilitate the free flow of personal data between Malta and any other Member State.[43] The DPA also provides a list of disqualifications to hold office as Commissioner, for e.g. if s/he is a Minister or a Member of the House of Representatives, or a judge or magistrate of the courts of justice.[44] The IDPC must have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform his or her duties and exercise his or her powers in accordance with article 53(2) GDPR.[45]

In the exercise of his tasks and powers, the Commissioner acts with complete independence and is free from external influence, whether direct or indirect, and must neither seek nor take instructions or direction from any person or entity.[46] Any officers or employees of the Commissioner are chosen by the Commissioner and are subject to his exclusive direction.[47]

The IDPC has a separate and distinct legal personality and is capable of entering into contracts, of acquiring, holding and disposing of any kind of property for the purposes of his tasks and powers, of suing and being sued, and of doing all such things and entering into all such transactions as are incidental or conducive to the effective performance of his tasks and exercise of his powers.[48]

The tenure of office of the IDPC is of five years and he is eligible for reappointment on the expiration of his term of office.[49] The Commissioner may not be removed from his office except by the Prime Minister upon an address of the House of Representatives supported by the votes of not less than two-thirds of all the members thereof and praying

41 Webpage: https://idpc.org.mt/en/Pages/Home.aspx.
42 Art. 11(1) DPA.
43 Art. 11(2) DPA.
44 Art. 11(3) DPA.
45 Art. 11(4) DPA.
46 Art. 12(1) DPA.
47 Art. 12(3) DPA.
48 Art. 13(1) DPA.
49 Art. 14(1) DPA.

for such removal on the ground of proved inability to perform the duties of his office (whether arising from infirmity of body or mind or any other cause) or proved misbehaviour.[50]

The Commissioner performs the duties assigned to him under the DPA and the GDPR and the functions assigned to him under the Freedom of Information Act[51] and any other law.[52] S/he has the power to institute civil judicial proceedings in cases where the provisions of the DPA or the GDPR have been or are about to be violated.[53] The IDPC may seek the advice of, and may consult with, any other competent authority in the exercise of his/her functions under the DPA and the GDPR.[54]

It has been reported that, for the period 25 May 2018 to 28 January 2019, in Malta, over one hundred (100) personal data breaches were notified to the IDPC, with seventeen (17) GDPR fines being imposed by the same. Per capita, the Maltese figures are significant.[55]

Question 10

The Office of the IDPC informed the author that all complaints received by the Office are investigated and that the degree of investigation may depend on the nature of the case, but as such no 'selective to be effective' approach is taken.[56]

Question 11

On 18 February 2019 the IDPC issued a decision to the Lands Authority after concluding an investigation of a data breach, that was brought to his attention by the media.[57] The findings of the investigation established that the online application platform available on the Authority's web portal lacked the necessary technical and organisational measures to ensure the security of processing. The Lands Authority was found to have infringed the provisions of article 32 GDPR and, in terms of article 21 DPA was served with an administrative fine of 5,000 euro. The level of the fine was stated to have been reached

50 Art. 14(2) DPA.
51 Chapter 496, Laws of Malta.
52 Art. 15(1) DPA.
53 Art. 15(2) DPA.
54 Art. 15(3) DPA.
55 DLA Piper GDPR data breach survey, www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/.
56 Meeting at the Office of the IDPC held on 23 May 2019.
57 'Massive Lands Authority security flaw dumps personal data online', Times of Malta, 23 November 2018 www.timesofmalta.com/articles/view/20181123/local/massive-lands-authority-security-flaw-dumps-personal-data-online.694982.

after the Commissioner took into account the circumstances set out under article 83(2) GDPR. The temporary ban imposed on the Authority's web portal was lifted. It was stated that the Lands Authority offered their full and unrestricted collaboration to the IDPC during the course of the entire investigation.[58]

Article 21 DPA implements article 83(7) GDPR and provides that the IDPC may impose an administrative fine on a public authority or body of up to 25,000 euro for each violation and additionally 25 euro for each day during which such violation persists, which fine shall be determined and imposed by the IDPC in accordance with the procedure stipulated in article 26 DPA, for an infringement under article 83(4) GDPR.

The fine that the IDPC may impose on a public authority or body for an infringement of article 83(5) or (6) GDPR (in accordance with the same procedure under article 26 DPA) must not exceed 50,000 euro for each violation and additionally 50 euro for each day during which such violation persists. Administrative fines on a public authority or body are to be imposed by the IDPC after giving due regard to the circumstances of the case pursuant to article 83(2) GDPR.

Further to the GDPR, article 22 DPA provides that any person who – (a) knowingly provides false information to the IDPC when so requested by the IDPC pursuant to his investigative powers under article 58 GDPR, or any other law; or (b) does not comply with any lawful request pursuant to an investigation by the IDPC – shall be guilty of an offence and shall, upon conviction, be liable to a fine (*multa*) of not less than one thousand, two hundred and fifty euro (1,250) euro and not more than fifty thousand (50,000) euro, or to imprisonment for six months, or to both such fine (*multa*) and imprisonment.

Question 12

Malta's legal system awards damages for intangible harm in some areas, most notably in cases dealing with human rights, defamation and intellectual property law. Save for a recently introduced exception,[59] the right of the plaintiff in an ordinary tort action to recover damages for intangible harm is not acknowledged by statute in Malta. When awarding damages for intangible harm (termed 'moral damages' in the Maltese legal system), and in the absence of concrete evidence to calculate *damnum emergens*[60] and/or

58 Press release 'Lands Authority Personal Data Breach' Reference Number: IDPC011, 18 February 2019, https://idpc.org.mt/en/Press/Pages/Lands-Authority-Personal-Data-Breach.aspx.

59 See Act XXXII of 2018, article 15 (discussed below).

60 Actual damages sustained.

lucrum cessans,[61] the Maltese courts tend to use their discretion *arbitrio boni viri*[62] in establishing the amount of compensation to be awarded.

Civil damages

In Malta the courts have traditionally affirmed that moral damages are not awarded in an ordinary action for civil damages under the law of tort or quasi-tort, but admitted this possibility under human rights law.[63] However, this traditional position has been contested and challenged as this means that moral damages may be awarded against the State in a case brought before the Civil Court, First Hall (in its Constitutional jurisdiction),[64] and potentially appealed before the Constitutional Court, but not in a case brought against a private individual (or the State[65]) before the (ordinary) Civil Courts (First Hall, and potentially appealed before the Court of Appeal.) While the argument has been made for the horizontal effects of fundamental human rights (understood not as 'holding individuals responsible for human rights violations' but as 'keeping human rights principles in mind when judicially interpreting private law'),[66] this is not uncontroversial.[67]

In Busuttil v Muscat,[68] the Civil Court held that the aesthetic facial injury suffered by the applicant due to medical negligence violated the value of psycho-physical integrity which it held was protected by the Constitution of Malta, the ECHR and article 3 of the Charter ('Everyone has the right to respect for his or her physical and mental integrity.') Holding that the ordinary law must be interpreted in a manner that is 'constitutionally compliant', the Civil Court interpreted the Civil Code in this light. In particular, the Court focused on Articles 1033 and 1045 of the Civil Code:

> Any person who, with or without intent to injure, voluntarily or through negligence, imprudence, or want of attention, is guilty of any act or omission

61 Ceased/lost profits; losses of future earnings arising from any permanent incapacity, total or partial.

62 'According to the judgment of a fair man.'

63 For a fuller account see D.E. Zammit, 'How human rights have influenced Maltese civil liability jurisprudence', in R. Magion (Ed.), *The UN Declaration of Human Rights: 70 years on*, Malta, Fondazzjoni Celebrazzjonijiet Nazzjonali, 2018, p. 34; referencing C. Micallef Grimaud, 'Article 1045 of the Maltese Civil Code: Is Compensation for Moral Damage Compatible Therewith?', *Journal of Civil Law Studies*, Vol. 4, No. 2, 2011, pp. 481-513. Cf. also A. Wadge (2018) Moral Damages in Public Law with particular reference to remedies arising from Human Rights Action, Unpublished LLD dissertation, University of Malta.

64 Under art. 46 Constitution of Malta.

65 Cf. article 46(2) proviso, Constitution of Malta.

66 Zammit, 2018, p. 36.

67 See G. Bonello, 'Misunderstanding the Constitution – 2: Can individuals be sued for human rights violation?', Sunday Times of Malta, 14 January 2018, https://timesofmalta.com/articles/view/Misunderstanding-the-Constitution-2-Can-individuals-be-sued-for-human.667891.

68 Linda Busuttil illum Cordina et. v. Dr Josie Muscat et. Civil Court (First Hall), 30 November 2010.

> constituting a breach of the duty imposed by law, shall be liable for *any damage* resulting therefrom.[69]
>
> The damage which is to be made good (….) shall consist in the *actual loss* which the act shall have directly caused to the injured party, in the expenses which the latter may have been compelled to incur in consequence of the damage, in the loss of actual wages or other earnings, and in the loss of future earnings arising from any permanent incapacity, total or partial, which the act may have caused.[70]

The Court held that the words 'any damage' and 'actual loss' were broad enough to encompass damage to psycho-physical integrity as a justification for a compensatory damages award to the victim. It then proceeded, *arbitrio boni viri*, to compensate plaintiff by awarding 5,000 euro in damages, which were stated by the court to be non-patrimonial (that is to say, 'moral') in character.

However, the Court of Appeal in Fenech & Others v Malta Drydocks[71] and subsequent cases[72] did not follow the same approach to human rights envisaged in Busuttil v Muscat, which itself was revoked on appeal.[73] In the latter judgment, the Court of Appeal reiterated the orthodox position, simultaneously affirming the non-compensability of moral damage in the context of ordinary civil liability litigation and the adequacy and sufficiency of the compensation thus granted, even understood as an ordinary remedy for a human rights violation.

Harm to the patrimony (civil damages) in Malta is quantified, where *lucrum cessans* damages are concerned, by means of the orthodox multiplier/multiplicand formula.[74] In the aforementioned judgments, it appeared to be the settled position of the Maltese courts that moral damages, provided they were expressed in terms of the categories of compensable patrimonial damages, were rendered *indirectly* compensable. This usually required the individual judge to interpret the applicable heads of damage flexibly enough, to incorporate or exclude particular forms of non-patrimonial damage according to his or her sense of what was required to achieve a *restitutio in integrum*[75] in the case at hand and by relying

69 Art. 1033 Civil Code. Emphasis added.

70 Art. 1045 Civil Code. Emphasis added.

71 Court of Appeal, 3 December 2010, Writ Number 1427/1997.

72 See for e.g. John Mary Abela et. v. Policy Manager tal-Malta Shipyards fi hdan il-Ministeru ghall-Infrastruttua, Trasport u Komunikazzjoni noe. et. Constitutional Court, 11 April 2011, Writ Number 25/2009/1.

73 Linda Busuttil et. v. Dr Josie Muscat u Tania Spiteri, delivered by the Court of Appeal on 27 June 2014, Writ Number 2429/1998/1.

74 Cf. Grech Trevor vs Agius Lawrence, Civil Court, First Hall, 17 October 2018, Reference 1030/2013, Mr Justice Grazio Mercieca (currently under appeal). See also C. Bugeja, 'The court's calculator', Times of Malta, 11 February 2019, https://timesofmalta.com/articles/view/the-courts-calculator.701658.

75 'Full restitution', that is that an injured party is, through the awarding of damages, restored to the state which would have prevailed had no injury been sustained.

on the court's discretion to adapt its damages awards to the particular circumstances of the case before it under article 1045(2) Civil Code:

> The sum to be awarded in respect of such incapacity shall be assessed by the court, having regard to the circumstances of the case, and, particularly, to the nature and degree of incapacity caused, and to the condition of the injured party.

The developing *status quo* was dramatically impacted by *Brincat and others v Malta*,[76] a case which concerned ship-yard repair workers who were exposed to asbestos for a number of decades beginning in the 1950s to the early 2000s which led to them suffering from asbestos related conditions. The ECtHR held that the non-compensability of moral damage in the context of ordinary civil liability litigation (for damages arising out of tort or contractual liability) meant that access to a human rights remedy could no longer be denied whenever an alleged victim of a human rights violation sued the Government for compensation of moral damages. The ECtHR ordered the payment of non-pecuniary ('moral') damages to the applicants/victims.

A further development occurred in the case of Agius v the Attorney General et, which concerned the death of an inmate at Malta's main prison resulting from an incorrect administration of methadone to a drug addict. In this case, following the case being tried before the Civil Court and the Court of Appeal,[77] a Constitutional case was filed.[78] On appeal, the Constitutional Court[79] held that since Articles 1045 and 1046 of the Civil Code fall under the sub-title 'Of Torts and Quasi-Torts', it is clear that any prohibition of the award of moral or non-patrimonial damages could only apply to actions in tort or quasi-tort. The Constitutional Court's classification of the action in this case as originating from a breach of a contractual and/or legal (*ex lege*) relationship does evoke an uncomfortable future scenario in which non-patrimonial damage will only be compensated if the underlying relationship can be construed as contractual or legal, and not if it is understood as tortious.[80]

As aforementioned, in 2018 the Civil Code underwent some amendments, including the addition of a proviso to article 1045(1), which provides that 'in the case of damages arising from a criminal offence, other than an involuntary offence, (…) the damage to be

76 *Brincat and Others v. Malta*, ECHR 232 (2014) Applications Nos 60908/11, 62110/11, 62129/11, 62312/11, and 62338/11.

77 Civil Court, First Hall, 6 October 2010; Court of Appeal, 1 April 2014.

78 Civil Court, First Hall (Constitutional Jurisdiction), 15 January 2015, Reference 33/2014.

79 Jane Agius v. the Attorney General, the Minister for the Interior and National Security and the Honourable Prime Minister, Constitutional Court, 14 December 2015, Writ number 33/2014/1.

80 Zammit, 2018, p. 61.

made good shall also include any *moral harm and, or psychological harm* caused to the claimant.'[81] (my emphasis)

Zammit opines that this recent enactment, while introducing the explicit right of the plaintiff in an ordinary action in tort to recover moral and/or psychological damages (within the parameters set out therein), may have (possibly, unintended) consequences insofar as the proviso may be interpreted to mean that moral and/or psychological damages may now only be (expressly) awarded within the limits contemplated in the said proviso, but not in all cases, for e.g. where the harm is caused by an involuntary offence; thus foreclosing potential further judicial developments particularly in light of the effects of judgments by the Constitutional Court awarding moral damages in, for example, the asbestosis cases.[82]

Other specific branches of Maltese law

An award of damages may be regulated by a specific branch of Maltese law outside the ambit of the Civil Code; namely: human rights cases, the Media and Defamation Act,[83] the Enforcement of Intellectual Property Rights (Regulation) Act,[84] the Consumer Affairs Act,[85] the Promises of Marriage Law,[86] and, of course, the DPA. For example, in proceedings instituted under the Media and Defamation Act, the Court may order the defendant to pay a sum not exceeding eleven thousand, six hundred and forty eruo (11,640 euro) by way of *moral damages* in addition to actual damages; in actions for slander the maximum amount to be awarded by way of moral damages is five thousand euro (5,000 euro).

Intellectual Property law

In intellectual property cases, a court that concludes that the defendant has knowingly engaged in infringing activity will order the payment of damages to the rightholder 'commensurate with the actual prejudice suffered by the said rightholder as a result of the infringement':

> In setting the amount of damages due, the Court *shall* take into account all relevant aspects, including all the negative economic consequences that may have been suffered by the injured party including lost profits, as well as any unfair profits made by the infringer and, *where it deems appropriate*, other

81 Added by Act XXXII.2018.15.
82 G. Caruana Demajo et al, (2018) XVIII. Malta, in E. Karner et al. (Eds), European Tort Law Yearbook, Vol. 7, No. 1 (2018), p. 372.
83 Chapter 579 Laws of Malta.
84 Chapter 488 Laws of Malta.
85 Chapter 378 Laws of Malta.
86 Chapter 5 Laws of Malta.

> elements such as the *moral prejudice* caused to the rightholder by the infringement:
> Provided that instead of the above method of calculation of damages, the Court may, *where it so considers appropriate*, choose to apply an alternative method of calculation involving the setting of a lump sum of damages payable which shall include elements such as at least the amount of royalties or fees which would have been due had the infringer requested authorisation to use the intellectual right in question.[87] (emphasis added by author)

Therefore, the Court has the discretion to award damages on an *arbitrio boni viri* basis under both article 12(2) and article 12(2) proviso (quoted above). It is unclear under which of these methods the Court has wider discretionary powers; in particular whether moral prejudice and/or similar elements are precluded from being included in the lump sum that can be awarded by the Court under the proviso to article 12(2).[88]

Article 12(2) is one of the few instances in Maltese law where moral prejudice is explicitly taken into consideration when liquidating damages. One of the first IP judgments to award damages invoking moral prejudice explicitly is the case Air Malta P.L.C. vs Efly Company Limited.[89] However, this was done on an *arbitrio boni viri* basis and therefore no explanation of the methods of calculation in question were entertained by the Court.

In the case Av. Dottor Antoine Camilleri noe (acting as special mandatory for and on behalf of Bacardi & Company Limited) vs Patrick Cellars Limited,[90] the court – in a case concerning the 'exhaustion of rights'/ trademark infringement by importing/ commercialising goods in Malta which were not destined for the EU/EEA market – liquidated the damages caused to Bacardi, in terms of article 12, in the amount of fifty-two thousand six hundred and fifty (52,650) euro in damages, including thirty thousand euro (30,000) euro in other damages (particularly 'moral damages', which include reputational damage). The Court stated that it was applying article 12(2)proviso and, having taken into consideration all the aspects of the case, awarding *arbitrio boni viri* the global amount of 30,000 euro in other damages.

87 Art. 12(2), Enforcement of Intellectual Property Rights (Regulation) Act, Chapter 488 Laws of Malta; transposing the provisions of Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L157/45.

88 C. Micallef Grimaud, 'Damages in Maltese Intellectual Property Cases: A Brief Look at Article 12 of Chapter 488 of the Laws of Malta', Mamo TCV Advocates, 25 March 2014 https://www.mamotcv.com/resources/news/damages-in-maltese-intellectual-property-cases-a-brief-look-at-article-12-of-chapter488-of-the-laws-of-malta.

89 Air Malta PLC (C-2685) vs Efly Company Limited (C-46370) – 30 March 2010 – First Hall, Civil Court.

90 Civil Court, First Hall, 19 May 2015 (Application No. 406/2011).

In Av. Dottor Antoine Camilleri noe (acting as special mandatory for and on behalf of Nando's Limited) vs Mirale and Lamare Limited,[91] the court awarded ten thousand euro (10,000 euro), with interest running from the data of the filing of the case, in moral damages calculated on the basis of *arbitrio boni viri* for the breach of rights suffered.

The onus of conducting an assessment *arbitrio boni viri* is placed upon the judge as the learned professional capable of delivering an amount based on equity. The author has been unable to trace any judgment of our courts which specifies in further detail how damages for 'moral prejudice' are calculated/ quantified/ liquidated in terms of article 12, since in the case-law identified no further deliberations were specifically entertained by the Courts on this point.

Data Protection law

Article 30(1) DPA states: 'Without prejudice to any other remedy available to him (…), a data subject may, where he believes that his rights under the GDPR or this Act have been infringed (…) by sworn application filed before the First Hall of the Civil Court, institute an action for an effective judicial remedy against the controller or processor concerned. (2) A data subject may also, by sworn application filed before the First Hall of the Civil Court, institute an action for damages against the controller or processor who processes personal data in contravention of the provisions of the GDPR or this Act.'

The DPA also explicitly provides in article 30(3) that 'If in determining an action [for damages] the court finds that the controller or processor is liable for the damage caused pursuant to Article 82 of the [GDPR], the court shall determine the amount of damages, including, but not limited to, *moral damages* as the court may determine, due to the data subject.'[92]

There are so far no decided cases awarding damages for intangible harm in the area of data protection law.

Question 13

Malta has to the best of this author's knowledge not introduced any legislative measures intended to facilitate representative actions pursuant to article 80 GDPR. Neither have any such representative actions been brought in practice.

A 'representative action', defined as 'proceedings that are brought on behalf of a number of class members by a representative body', is possible according to the provisions of the Collective Proceedings Act,[93] enacted in 2012 – *but* only with regard to an infringement

91 Civil Court, First Hall, 13 June 2019 (Application No. 853/2017).
92 Emphasis added.
93 Laws of Malta, chapter 520.

of the Acts listed in Schedule A of the Act, i.e. the Competition Act,[94] and articles 101 or 102 TFEU, the Consumer Affairs Act[95] and the Product Safety Act.[96] In a representative action, the Court shall approve a registered consumer association or a 'constituted body' to act as a class representative according to the terms of article 12(1) of the Act. In this author's opinion, the DPA and the GDPR should be brought within the purview of this Act.

MITLA[97] has reacted to certain developments at the local level, for example with regard to the government's announced plans to introduce public, smart CCTV surveillance cameras (with facial recognition technology) in selected locations in Malta to address "ant-social behaviour" hotspots.[98] MITLA has also pronounced itself on the matter of the erasure of criminal court judgements from the publicly accessible online judgments database.[99] This author believes that in principle MITLA should qualify to bring a representative action in terms of Article 80(1) GDPR.

Question 14

Malta has recently established a new authority – the Malta Digital Innovation Authority[100] – to regulate innovative technologies. However the scope of this authority is limited to certifying the functionality of 'innovative technology arrangements' and does not extend to dealing with complaints relating to data protection. Any data protection issues in the application of any innovative technology arrangement would need to be referred to the Office of the IDPC.

94 Laws of Malta, chapter 379.

95 Laws of Malta, chapter 378.

96 Laws of Malta, chapter 427.

97 MITLA is registered as a Voluntary Organisation (VO/1166) in terms of art. 3 of the Voluntary Organisations Act 2007 (Act No, XXII of 2007), Malta.

98 MITLA, 'Specific laws are required for mass-scale facial recognition applications', 7 December 2017, www.mitla.org.mt/specific-laws-required-mass-scale-facial-recognition-applications/. Reported in the news: M. Vella, 'IT experts warn of greater privacy risks with facial recognition CCTV: Plans for facial recognition CCTV in Paceville require new rules to safeguard fundamental rights, Malta IT law association says', MaltaToday, 7 December 2017, www.maltatoday.com.mt/news/national/82918/it_experts_warn_of_greater_privacy_risks_with_facial_recognition_cctv#.XS7f5i2Q1sM; M. Vella, 'Facial recognition CCTV for Paceville and Marsa by 2019: The facial recognition software is expected to be deployed in Paceville and Marsa, after data protection concerns are addressed with the Information and Data Protection Commissioner', MaltaToday, 22 October 2018, www.maltatoday.com.mt/news/budget-2019/90331/facial_recognition_cctv_for_paceville_and_marsa_by_2019#.XS7gFi2Q1sM. Cf. also: F. Zammit, 'Safe City Malta': Is Privacy the Real Crux of the Matter?', Isles of the Left, 16 January 2019, www.islesoftheleft.org/safe-city-malta-is-privacy-the-real-crux-of-the-matter/, expressing concern about potential uses of data collected from smart CCTV surveillance for social profiling and resultant discrimination.

99 See above response to question 7.

100 Established by the Malta Digital Innovation Authority Act, chapter 591 Laws of Malta, mdia.gov.mt.

Cooperation between the Office of the IDPC and other regulators has to date been informal and on an *ad hoc* basis.[101]

D Data Processing for National Security Purposes

Question 15

In Malta communications data is retained according to the provisions of S.L. 586.01 Processing of Personal Data (Electronic Communications Sector) Regulations. Article 19(1) states that 'Data retained under this Part shall be disclosed only to the Police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime.'

The closest to a definition of the Security Service of Malta is that found in article 3 of the Security Service Act,[102] as follows:

1. There shall continue to be a Security Service … under the authority of the Minister.
2. The function of the Service shall be to protect national security and, in particular, against threats from organised crime, espionage, terrorism and sabotage, the activities of agents of foreign powers and against actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
3. It shall also be the function of the Service to act in the interests of – (a) the economic well-being of Malta; and (b) public safety, in particular, the prevention or detection of serious crime.

Subsidiary legislation 586.09 Restriction of the Data Protection (Obligations and Rights) Regulations, article 4(4), provides: 'Any restriction to the rights of the data subject referred to in article 23 GDPR shall only apply where such restrictions are a necessary measure required:(a) for the safeguarding and maintaining of *national security*, public security, defence and the international relations of Malta; …'[103]

It is unclear whether our national authorities accept the application of the Charter to data retention for national security purposes as the issue has never really been a controversial matter in this country.

101 Discussion/interview held at the Office of the IDPC on 23 May 2019.
102 Chapter 391, Laws of Malta.
103 Emphasis added.

The Netherlands

Dominique Hagenauw and Hielke Hijmans[*]

A Setting the Scene

Question 1

The main national legal instrument introduced to implement the General Data Protection Regulation (hereinafter "GDPR") in The Netherlands is the GDPR Implementation Act (in Dutch: *Uitvoeringswet Algemene verordening gegevensbescherming,* hereinafter "UAVG"). It was published in the Official Journal of the Kingdom of the Netherlands on 22 May 2018[1] and applies as of 25 May 2018.[2] The Netherlands therefore completed their main legislative procedure for the GDPR just in time.[3]

The UAVG revokes the former Dutch personal data protection act (in Dutch: *Wet bescherming persoonsgegevens*, hereinafter "Wbp"), it re-establishes the institution and powers of the Dutch supervisory authority, the Autoriteit Persoonsgegevens (hereinafter AP),[4] and it supplements the GDPR by including certain derogations from the GDPR and by using so called opening clauses where the GDPR left some discretion to individual Member States.[5]

The GDPR Adaptation Bill (in Dutch: *Aanpassingswet Algemene verordening gegevensbescherming*, hereinafter "Adaptation Bill") – published in the Official Journal on

---

* Dominique Hagenauw: Independent Expert on privacy and the protection of personal data; Data Protection Officer at Vrije Universiteit Amsterdam (until March 2020); previously Principal Legal Advisor at Considerati and Senior International Officer at the Dutch Data Protection Authority. Hielke Hijmans: President of the Litigation Chamber of the Belgian Data Protection Authority; Researcher at Vrije Universiteit Brussels; Member of the Meijers Committee. With contributions of Christiaan van Dissel, Sophie van der Hoeven-Bots, Violet Mantel, Olga Nijveld, Edmon Oude Elferink, Barbara Schenk, Merle Temme, Sybe de Vries and Martine Wijers.

1 UAVG, www.officielebekendmakingen.nl/stb-2018-144.html. All webpages referred to were last visited on 19 June 2019. On the UAVG, see Hielke Hijmans, De AVG en de UAVG: Het grondrecht op gegevensbescherming wordt door de EU beschermd. De werking van dit recht in de Nederlandse rechtsorde roept vragen op, *NJB* 2018, afl 7.

2 Royal Decree, www.officielebekendmakingen.nl/stb-2018-145.html.

3 P. Breitbarth, "The GDPR Implementation in the Netherlands", p. 1, https://blogdroiteuropeen.files.wordpress.com/2018/06/paul-1.pdf.

4 Website AP, www.autoriteitpersoonsgegevens.nl/en/node/1930. See answers to questions 9-11.

5 Articles allowing for the Member States to derogate are sometimes referred to as "opening clauses".

27 July 2018[6] – adapts existing references to the previous data protection legislation in a number of legislative acts in the Netherlands.

In implementing the GDPR, the Netherlands has refrained from making policy decisions where this would lead to a shift from the former data protection regime under the Wbp. Instead, the idea was to retain existing national standards and maintain the *status quo* as much as possible in order to enable a smooth transition to the new regime.[7]

This approach is referred to as "policy-neutral", consistent with the general approach in the Netherlands when implementing EU legislation.[8] Before making decisions to deviate from the *status quo,* the Dutch legislator intended to gain some experience with the GDPR for a number of years first.[9]

Existing national particularities, such as a stringent restriction on the use of social security numbers,[10] the treatment of data related to criminal behaviour as "special" personal data[11] and the minimum age for consent of 16,[12] have thus been retained. Especially the latter point, the age at which children can consent independently, is being debated extensively in the Netherlands.[13]

Concerning the articles specifically mentioned in the question:[14]

- Article 6 GDPR, including article 6(1)(c) has not been separately implemented in the Netherlands.[15]
- With regard to article 23 GDPR, this has been implemented in articles 41, 42 and 47 UAVG.
  - Article 41 UAVG is almost exactly the same as article 23 GDPR, with one interesting deviation: the UAVG does not allow for the restriction of articles 22 and 5 GDPR.[16]

6 Adaptation Bill, https://zoek.officielebekendmakingen.nl/stb-2018-247.html.
7 EM UAVG, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.
8 P. Breitbarth, "The GDPR Implementation in the Netherlands", p. 4, https://blogdroiteuropeen.files.wordpress.com/2018/06/paul-1.pdf.
9 EM UAVG, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.
10 Art. 46 UAVG.
11 Art. 31, UAVG.
12 Art. 5(1) UAVG.
13 Letter of 1 April 2019 (32761, nr. 132), p. 12.
14 EM UAVG, Implementation table (*Implementatietabel*), p. 70, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.
15 EM UAVG, p. 29, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.
16 EM UAVG, p. 106, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

  - Article 42 UAVG provides that article 34 GDPR is not applicable to financial operators.[17]
  - Article 47 UAVG creates exceptions to the rights of data subjects with regard to public registers.[18]
- The use of social security numbers has been under a strict regime before, and article 46 UAVG stipulates that national identification numbers may only be used when explicitly provided for by law.[19]

The policy-neutral approach of the Dutch legislator has been subject to criticism. The Dutch parliament requested the government to make an inventory on a number of issues and take action where necessary.[20] Examples are the processing of data by smaller organizations (such as charities, sports associations, church communities and others), the processing of personal data at work in the event of sickness and the minimum consent age for children. In a letter of 1 April 2019[21] the minister for Legal Protection addressed and evaluated these concerns. Legislative steps to change the UAVG regarding some of these issues are being investigated.

Question 2

Article 10 of the Constitution for the Kingdom of the Netherlands[22] contains the fundamental right to respect for one's private life (in Dutch: *persoonlijke levenssfeer*).[23] The article has been introduced in the Constitution in 1983. Article 10 of the Constitution also instructs the legislator to create rules protecting private life relating to the recording and provision of personal data, the right to be informed, the right to have access to such data and to have it corrected.

The preamble of the UAVG, governing the protection of personal data, explicitly refers to article 10 of the Constitution.

17 EM UAVG, p. 106, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

18 Art. 21 GDPR (*Right to object*) is declared as generally not applying to public registers. Articles 15 GDPR (*Right of access by the data subject),* 16 GDPR (*Right to rectification*), 18 GDPR (*Right to restriction of processing*) and 19 (*Notification obligation regarding rectification or erasure of personal data or restriction of processing*) GDPR do not apply insofar as a special procedure has been established by law.

19 In other cases article 46 UAVG also allows for deviation by general administrative order (*Algemene maatregel van Bestuur*) but also then no purpose for processing are acceptable which are incompatible with the original purpose for which the number has been processed (art. 5(1)b GDPR).

20 Motie Koopmans (34851, nr. 19) of 8 March 2018.

21 32761, nr. 132.

22 Constitution of The Netherlands, https://zoek.officielebekendmakingen.nl/stb-2019-33.html.

23 D.E. Bunschoten, commentaar op artikel 10 Grondwet, in: Tekst & Commentaar Grondwet en Statuut, Deventer: Kluwer 2018.

Article 13 of the Constitution is also worth mentioning in relation to the protection of personal data, as it addresses the secrecy of correspondence, telephone and telegraph. An amendment aimed at broadening the scope of article 13 to "newer" kinds of communication has already been approved by both Chambers of the Dutch parliament.[24] For the amendment to come into force, the proposal to change the Constitution must be confirmed again by both Chambers after a general election has taken place.

A particularity of the Dutch Constitution is that no constitutional review of formal laws is possible. Article 120 of the Dutch Constitution provides that no judge will rule on the constitutionality of laws and treaties (in Dutch: *toetsingsverbod*).[25]

However, regulations of lower administrative bodies may be tested against the Constitution by the courts. Also, article 94 of the Dutch Constitution does allow for any law to be tested against any self-executing treaty. The ECHR is the treaty most commonly tested against by Dutch courts in this context.

Where appropriate, Dutch courts have in the past referred to Article 8 ECHR, because they could not directly invoke article 10 of the Constitution. In recent years, Dutch courts increasingly refer to articles 7 and 8 of the Charter.

In two Dutch cases where Article 8 of the Charter played a role, albeit in addition to article 8 ECHR.[26] Both were high-impact cases which eventually reached the Supreme Court of the Netherlands (in Dutch: *Hoge Raad*):

- An action by several individual citizens and an NGO (Privacy First) was brought against an amendment to the Passport Act, which obliged citizens to provide their fingerprints to be added to their travel documents. According to Privacy First, this requirement was contrary to Article 8 ECHR and Article 8 Charter.[27] Privacy First held that the creation of a central registry, the central storage (or not) of the data, the regime of providing data to others, the lack of necessary additional rules, the infringements on the principles of proportionality and subsidiarity and the amount of purposes for which the personal data would be stored, led to the new rules being unjustified. Eventually, the case was not resolved on the merits. The Supreme Court dismissed the case in 2015 due to a lack of standing of both Privacy First and the individuals concerned.
- The association of practicing General Practitioners (GPs) brought a case against a newly established system allowing for the (far-reaching) electronic processing of medical

24 Proposal to change the Constitution, www.eerstekamer.nl/behandeling/20170914/publicatie_wet_2/document3/f=/vkhlc89peuxz.pdf.

25 Nor does the Netherlands have a Constitutional Court.

26 Cases which referred to article 7 of the Charter generally concern criminal law, immigration law and social security law-issues and are therefore not further elaborated on.

27 ECLI:NL:HR:2015:1296, 22 May 2015, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2015:1296.

personal data in the Netherlands.[28] The system would allow primarily for GPs[29] to access personal data of a patient, in addition to a "professional summary" created on the basis of the GP's own patient file. This system, according to the association, unnecessarily infringed upon patients' rights to privacy, specifically article 10 of the Dutch Constitution, article 8 ECHR and article 8 Charter.[30] The *Hoge Raad* however agreed with previous instances that the proportionality and subsidiarity were sufficiently respected.

Both cases were decided before the GDPR came into effect, which means that it cannot be said with certainty that future cases invoking article 8 of the Charter will be assessed similarly by Dutch courts.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

In the Netherlands the interpretation of the principles of fair processing, purpose limitation and data minimisation varies strongly per sector, hence no 'one true answer' can be given for their application, but some examples are worth mentioning.

In June 2018, the AP has looked into the processing by the Netherlands Tax and Customs Administration of the national identification number (BSN) in the VAT-identification numbers of freelancers.[31] The AP states in its final report that by converting the BSN and using it as (part of the) VAT-identification number, the BSN is used improperly as this would result in essence that a person is forced to reveal his or her BSN publicly and to third parties, in violation of the UAVG and the principles of fair and lawful processing of article 5(1)(a) of the GDPR. The Dutch Tax and Customs Administration is required to take measures to address the situation before 1 January 2020.

28 ECLI:NL:HR:2017:3053, 1 December 2017, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:3053.

29 Thus GPs who are temporarily filling in for the patient's own GP.

30 Another main complaint brought forward by the association was that the system relied on consent of the patient as a legal basis for processing (as opposed to an obligation established by law) and could, on that ground, not provide a basis for infringing medical confidentiality. It is worth noting that a legal proposal which intended to create a proper legal framework for such as system had been rejected by the Dutch Senate in 2011.

31 "Onderzoek naar de verwerking van BSN in btw-identificatienummers door de Belastingdienst", Autoriteit Persoonsgegevens, June 2018.

Another interesting example concerns the Dutch system of credit registration. Credit providers are obliged to take part in a system of credit registration and need to register credits above € 250. Whenever a debtor doesn't commit to paying instalments, that person gets a 'negative registration' in the system. The information in the system can be used by new credit providers to determine whether the consumer has a financial situation (un)suitable for a newly requested credit. There are a myriad of court cases against the credit providers registering a consumer in the system concerning their negative registrations, which consumers become aware of when learning that they are not eligible for new credits and mortgages as a result of these negative registrations.

In 2011, the Dutch Supreme Court ruled that the registration should at all times be in accordance with the principles of proportionality and subsidiarity.[32] It further held that under certain circumstances it may not be the negative registration itself, but the minimum registration period of five years, that is disproportionate with regard to the purpose of the processing of the data, which is combating over-crediting consumers and protecting credit providers from financial risks.

Question 4

Similar to the answer to question 3, there is no 'one true answer' for the use of the legal grounds of legitimate interest and consent. There are nevertheless interesting cases to be mentioned.

First of all, a recent ruling from a local court reaffirms the use – under certain conditions - of the legal ground of legitimate interest for processing personal data by using security cameras.[33] In the case at hand, the security camera was only recording a small part of a public road and people walking there would not be recorded fully. The owner of the camera demonstrated that less-intrusive security means were not sufficient to protect his property and the people and goods on it. Recording of images was needed to support any filing to the police. Moreover, people were informed that a security camera was recording and the owner of the security camera had verified its compliance with necessary safeguards. These reasons led the Court to rule that the "legitimate interest" could be used in this case.

With regard to the legal ground of consent, a relevant court case is on the national linking point for patient data ("LSP").[34] Following concerns of doctors, a case went up to the Supreme Court on whether the consent of a patient who needs medical attention would be sufficient to allow access to his or her medical record in case the doctor who had received

32 HR 9 September 2011, NJ 2011/595.

33 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2019:2725.

34 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:3053&showbutton=true&keyword=ECLI%3aNL%3aHR%3a2017%3a3053.

the consent and kept the record was not available. The Supreme Court upholds judgements of the lower courts in affirming that the patient's consent did sufficiently meet the requirements of freely given, specific and informed sufficiently and could therefore be relied upon for accessing and processing personal data of patients in absence of their "regular" doctor.

Question 5

In the Netherlands the debate on the validity of personal data as a counter-performance for the provision of digital content is not only related to the GDPR, but also to consumer law, especially the Digital Content Directive.

Even though there is no clear indication that public debate in the Netherlands mostly opposes to the use of personal data as counter-performance *per se,* both Chambers of the Dutch Parliament have put questions to the government concerning the lack of clear coordination between the Directive and the GDPR.[35]

The discussion inter alia revolved around which would be the correct lawful basis for processing personal data to deliver digital content, mainly focusing on whether this can only be the consent of person concerned or whether also other legal grounds would be possible.

Another important question that was raised is whether personal data in case of terminating the agreement should be valued in money and whether the consumer as a consequence should be financially compensated. The Dutch government, without further explanation, simply states that this is not necessary. The organization should either return the personal data to the consumer, or, if this is not possible, pay money as a form of compensation. The problem observed in legal literature is whether industry can be burdened with potentially millions of euros in collective actions initiated by consumers.[36]

Question 6

Article 40 UAVG provides for exemptions from the prohibition on automated individual decision-making. These exemptions take into account that not all cases of automated decision-making pose high risks in terms of a potential discriminatory effect. For example, automated individual decision-making regarding 'closed' decisions, that are based on the fulfillment of objective requirements, do not inhibit a high risk. Think of processing income

35 file:///Users/gebruiker/Downloads/beantwoording-aanvullende-kamervragen-over-richtlijnvoorstel-levering-digitale-inhoud-en-diensten.pdf.

36 H. Schulte-Nölke, 'Personal data is not a counter-perfomance – Plea for a data driven rethinking of contract and consumer law', *Tijdschrift voor Consumentenrecht en handelspraktijken* 2018, nr. 2, p. 75.

data for taxation purposes or basing traffic fines on photographs in combination with license plates.

The article also provides for several safeguards. First, a controller can only apply these exemptions for processing based on article 6(1)(c) or (e) GDPR.[37] Furthermore, the controller needs to take adequate measures for the protection of personal data.

For controllers that are not administrative bodies, such appropriate measures shall have been taken if the right to human intervention, the data subject's right to express his or her views and the right to contest the decision, are safeguarded. Provided other adequate measures are being taken by the controller to safeguard the data subject's rights, freedoms and legitimate interests, the requirement of human intervention may be set aside.

For automated decision-making by a government institution, the General Administrative Law Act (in Dutch: *Algemene wet bestuursrecht*, hereinafter "Awb") is applicable, in addition to the GDPR. This general law provides for comparable safeguards and principles that must be taken into account in decision making, including the principles of diligence and proportionality. It also provides for a subject's right to appeal decisions.

In its letter to the House of Representatives of April 2019 regarding the first experiences with the UAVG[38] the government responded to the request of the Dutch Trade Association,[39] to create a more generous exemption to offer more options for innovation regarding new profiling-based techniques. The government stated it would uphold its decision not to include an exemption in the UAVG for automated decision-making using profiling-techniques. It held that the risk that group-characteristics are attributed to an individual whilst it is not 100% certain that this individual, although belonging to the group, also has those specific characteristics, in combination with automated decision-making, is considered too great a risk.

The government has furthermore informed The House of Representatives that a working group is creating guidelines for the transparency of algorithms used by the government as well as guidelines for informing the public about big data applications by the government. The government is also looking into the possibility to create extra legal safeguards for big data applications by the government.[40]

37 Processing necessary for compliance with a legal obligation to which the controller is subject or processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

38 TK 2018/19, 32 761, nr. 132.

39 VNO-NCW and MKB Nederland.

40 TK 2018/19, 26 643, nr. 601.

Question 7

After the *Google Spain and Google* ruling[41], Google immediately put in place a search removal form on its website and made available a Transparency Report.[42] Between May 2014 and May 2019, somewhat over 150,000 requests for delisting URLs were made by users in the Netherlands. Out of this total, 49,4% of requests were granted (about 3% higher than EU average). After 25 May 2018, the percentage of URLs that were delisted increased from 47,8% to 56,3%, an increase of almost 10%. This may be explained by the strong awareness campaign for privacy led by the AP and the government in the months prior to this date.

Consumers may also, instead of addressing search engines directly, turn towards the AP to act as an intermediary. The AP uses the guidelines of the Working Party 29 as well as conditions derived from national and EU case law to determine whether the listing of the URL after a search inquiry is justified. However, only 5% of all incoming complaints were requests for intermediary action.[43]

Between 2014 and July 2019, 24 cases can be found where the right to be forgotten was invoked before a Dutch court. Only in six of the 24 cases did the judge rule in favour of the plaintiff.

Question 8

Article 85 of the GDPR relating to processing of data for journalistic purposes and for academic, artistic and literary expressions is implemented in article 43 UAVG. Given the 'policy neutral' implementation of the GDPR in the UAVG, most of the exemptions that were already created in the Wbp still apply.[44] Thus, a majority of articles of the GDPR do not apply to the processing of personal data solely for journalistic purposes and for the purposes of academic, artistic or literary expression, including articles 9 and 10 of the GDPR concerning the prohibition to process special categories of data or data relating to criminal convictions and offences.

The fact that not all provisions of the GDPR are applicable to data processing for journalistic purposes or for the purposes of academic, artistic or literary expression, does not mean that the privacy of the subjects is not being weighed. First, the general provisions and basic principles of the GDPR are still applicable. Second, a balancing of the right of

41 Judgment of 13 May 2014 in Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González (*Google Spain and Google*),ECLI:EU:C:2014:317, 13 May 2014.

42 Transparency Report "*Search removals under European privacy lawi*", Google.

43 "Klachtenrapportage: facts & figures. Overzicht 25 mei tot 25 november 2018", Autoriteit Persoonsgegevens.

44 Arts 7(3) and 11(2), Chapter III, Chapter IV (with the exception of Articles 24, 25, 28, 29 and 32), Chapter V, Chapter VI and Chapter VII GDPR.

freedom of expression and the right to privacy in concrete cases will be executed by the court, taking into account the specific circumstances of the case.[45]

Furthermore, some new elements have been introduced to keep in line with jurisprudence, like the exemption to the right of the data subject to withdraw his or her consent at any time.[46] This would mean for example that, once permission has been given for publication of an interview, this can generally not be withdrawn.

The Board of Journalism (in Dutch: *Raad voor de Journalistiek*) and the Dutch Society of Journalists (in Dutch: *Nederlandse Vereniging van Journalisten*) both have a code of conduct. These contain guidelines on the proportionality of interferences with privacy for journalistic purposes.

C Domestic Enforcement of Data Protection Law

Question 9

The AP is established as the sole data protection supervisory authority of the Netherlands.[47] According to Dutch public law, the AP is an autonomous administrative authority (in Dutch: *zelfstandig bestuursorgaan,* hereinafter "ZBO") at the level of the central government; it is endowed with legal personality.[48] In the Netherlands, autonomous administrative authorities are authorities that have been vested with public authority, but are not hierarchically subordinate to a minister. These authorities are created for instance where strict regulations have to be applied in large numbers of many individual cases, where independent experts have to be called in to carry out quality checks, issue licenses or grants, or where independent experts have to monitor the implementation of regulations.[49]

General provisions on autonomous administrative authorities are included in the Autonomous Administrative Authorities Framework Act (in Dutch: *Kaderwet ZBO's*). This act creates a legal framework that deals with the responsibilities of the minister on the one hand and the administrative body on the other hand.[50] The minister responsible

45 De pers en privacy. Hoe verhoudt de AVG zich tot het juridisch kader voor de journalistiek? Noot bij Rechtbank Amsterdam, 12 oktober 2018, ECLI:NL:RBAMS:2018:7397 (Oudkerk/Sanoma).

46 An exemption to ar. 7(3) GDPR.

47 Art. 6(1) Implementation Act.

48 Art. 6(1) Implementation Act.

49 See also https://www.overheid.nl/english/about-the-dutch-government/what-government-consists-of/autonomous-administrative-authorities.

50 See also Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Evaluatie Kaderwet zelfstandige bestuursorganen 2012-2016, May 2018.

has a limited number of powers, like the power to approve the budget.[51] These matters are specified when a ZBO is set up. The minister is only responsible for using these powers and not for the decisions made by the ZBO itself.

In order to fully guarantee the independence of the AP, certain sections of the Kaderwet ZBO's do not apply to the AP. As a consequence, the Minister for Legal Protection does, inter alia, not have the power to lay down policy rules relating to the way in which the AP performs its tasks[52] and to annul decisions of the AP.[53]

Composition; appointment process for members and staff

The AP comprises of a Chair and two other members.[54] The Chair, who shall satisfy the requirements for appointment as a judge, and the other members of the AP are appointed by royal decree on the nomination of the Minister for Legal Protection.[55] The term of office for chairman and members of the AP is 5 years.[56] They can once be re-appointed for a term of another 5 years.[57] The AP has a Secretariat whose officials are appointed, promoted, disciplined, suspended and dismissed by the AP.[58]

Powers and duties

The Awb regulates the process of administrative decision-making in a general sense and provides a general framework for the right of appeal to an administrative court against the orders issued.[59] Chapter 5 of the Awb relates to administrative enforcement action by administrative authorities, including general rules for monitoring compliance by inspectors and for administrative sanctions. As a result, at a national level, both the Awb and the UAVG deal with powers of the AP.

Under the UAVG, the AP is competent to perform the tasks and exercise the powers that are conferred on supervisory authorities by or pursuant to the GDPR.[60] The members and the officials of the AP, as well as other persons designated by the AP, are responsible for monitoring compliance with the GDPR and with other relevant legislative provisions.[61]

---

51 Cf. Chapter 4, Division 1, Autonomous Administrative Authorities Framework Act. See also: www.overheid.nl/english/about-the-dutch-government/what-government-consists-of/autonomous-administrative-authorities.

52 Art. 13(1) Implementation Act.

53 Art. 13(1), ibid.

54 Art. 7(1), ibid.

55 Art. 7(3), ibid.

56 Art. 7(5), ibid.

57 Art. 7(6), ibid.

58 Art. 10(1), ibid.

59 See also: T. Barkhuysen et al, 'The Law on Administrative Procedures in the Netherlands', NALL 2012, april-juni, DOI:10.5553/NALL/.000005.

60 Art. 14(1) Implementation Act.

61 Art. 15(1), ibid.

As a result, the **investigative powers** with which 'inspectors' are empowered according to Chapter 5 of the Awb are also entrusted to the AP.[62]

The investigative powers granted to supervisory authorities by the GDPR closely resemble the investigative powers mentioned in the Awb. In some cases, the Awb seems to be more wide-ranging, for instance when it comes to the subject of the investigation. The Awb states that "everyone" shall be obliged to cooperate fully with a supervisor[63], whilst Article 31 of the GDPR stipulates only that the controller and the processor (or their representative) should cooperate with the authority. There seems to be no legal obstacle to combine the investigative powers granted by the Awb and the GDPR.[64]

In addition to the **enforcement powers** provided by the GDPR, the AP has extra enforcement powers pursuant to article 58(6) GDPR, in particular administrative enforcement orders, either under the threat of enforcement action by or on behalf of the AP itself (in Dutch: *last onder bestuursdwang*) or under periodic penalty payment (in Dutch: *last onder dwangsom*). The power to impose these orders is derived from the Awb.[65] With such an administrative order, the AP can for example order a controller to comply with the GDPR and the UAVG. If the controller fails to comply with the order within the prescribed time limit, a specified amount of money must be paid. Furthermore, the AP can order any company or person to cooperate with the AP.[66]

The UAVG also provides that the administrative fines of article 83 GDPR may be imposed on *public* authorities and bodies, using the option given in article 83(7) GDPR.[67]

Lastly, the Implementation Act provides the AP with the power to **mediate**. The interested party may file a request with the AP to mediate in or advise on his or her dispute with the controller in cases concerning articles 15-22 of the GDPR.[68] In 2018, the AP has mediated in 129 cases.[69] These cases mainly concerned requests to delist search results on a person's name in a search engine (see also question 7). In most cases the search results were delisted after mediation by the AP.

The AP is not only responsible for monitoring compliance with the GDPR and the UAVG, but also ensures compliance with – among others – the Elections Act (in Dutch: *Kieswet*), the Basic Registration of Persons Act (in Dutch: *Wet basisregistratie personen*) and the Dutch Acts implementing Directive (EU) 2016/680: the Police Data Act (in Dutch:

62 See also: V.N. Mantel et al, 'De (U)AVG en de Awb: toezicht, sanctionering en rechtsbescherming', JBplus 2019/01.
63 Art. 5:20 Awb.
64 See also: V.N. Mantel et al, 2019.
65 Art. 16(1) Implementation Act and arts 5:21 and 5:32 of the Awb.
66 Art. 16(2) Implementation Act.
67 Art. 18(1) Implementation Act in conjunction with art. 83(7) GDPR.
68 Art. 36(1) Implementation Act.
69 Annual Report 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf.

Wet politiegegevens) and the Judicial Data and Criminal Records Act (in Dutch: *Wet justitiële en strafvorderlijke gegevens).*

Question 10

The starting point for complaint handling is that the AP will investigate the subject matter of complaints to the extent appropriate.[70] The AP has published policy guidelines on how it will prioritize the handling of complaints lodged with it under the GDPR (*Beleidsregels prioritering klachtenonderzoek AP*).[71] According to these guidelines, the AP will **firstly** determine whether the complaint concerns the processing of personal data relating to the complainant[72], and whether basic desk research leads to the conclusion that there is a clear violation of the GDPR – or to the conclusion that it is clear there is no breach of the GDPR, in which case the complaint will be rejected.

As a general rule, according to Dutch administrative law, the AP is required to take legal action (by means of a reparatory sanction) when it establishes an infringement of the GDPR after receiving a complaint in writing, lodged by an interested party, aimed at enforcing compliance with data protection rules.[73]

However, if the AP is able to resolve a complaint successfully by – for instance – offering guidance to the controller (thus taking 'informal enforcement action'), after which the controller brings its processing into compliance and the complainant is satisfied, the AP will close the case.

If the desk research points out that an infringement of the GDPR might occur, but a more thorough investigation is necessary in order to come to more definitive conclusions, the AP will **secondly** determine whether there is reason for further investigation. Criteria include:

a. How harmful is the alleged violation for the individual(s)?
   This depends on nature of the personal data involved and on the nature of the alleged violation.
b. What is the broader social significance of the case, taking into account the areas of special focus the AP publishes on a regular basis?

70 Art. 57(1)(f) of the GDPR. See also O.S. Nijveld and W. van Steenbergen, 'Het Awb-landschap door een AVG-filter', TvT 2018-4, p. 95-102.

71 *Stcrt*. 2018, 54287.

72 Also a not-for-profit body, organisation or association that is active in the field of the protection of data subjects' rights and freedoms and can be considered an 'interested party' in terms of art. 1:2(3) Awb, independently of a data subject's mandate, has the right to lodge a complaint with the AP.

73 ABRvS 11 August 2004, *AB* 2004, 444 (m.nt. F.R. Vermeer).

The AP issues focal areas for the coming year,[74] and takes into account the number of individuals concerned and whether or not the complaint concerns cross-border processing.

c. To what extent will the AP be able to act effectively?
The AP will take into consideration other complaints filed with the AP, its available manpower and budget.

Question 11

Besides sanctions and corrective measures as referred to in article 58(2) GDPR and additional sanctions adopted at national level[75], the AP also uses 'informal' enforcement instruments to obtain compliance (for instance, in reaction to a complaint[76]). Examples may include meeting with a controller to offer guidance on a specific GDPR provision violated (in Dutch: *"normoverdragend gesprek"*) or issuing a guidance letter (offering guidance on compliance with the requirements of the GDPR).[77]

GDPR sanctions and additional sanctions

In 2018, the AP took enforcement actions against 17 private companies, public authorities and other organisations. The AP imposed sanctions in six cases, four of which are published:

- The AP imposed an administrative fine pursuant to Article 83 GDPR on Uber B.V. and Uber Technologies, Inc. of €600,000 for violating the data breach regulations.[78]
- The AP imposed a ban on processing as referred to in Article 58(2)(f) GDPR against the Netherlands Tax and Customs Administration which may no longer process the national identification number as part of the VAT number of self-employed persons (see further answer 3).[79]
- The AP imposed an administrative enforcement order under periodic penalty payment[80] – an additional sanction adopted at national level – against the Employee Insurance

74 See the Supervisory framework, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf, visited 2 August 2019.

75 See Question 9 on the additional enforcement powers provided for in the Implementation Act and the Awb.

76 See also Question 10.

77 Annual Report 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf.

78 'AP legt Uber boete op voor te laat melden datalek', https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-uber-boete-op-voor-te-laat-melden-datalek.

79 'Belastingdienst mag BSN niet meer gebruiken in btw-identificatienummer', https://autoriteitpersoonsgegevens.nl/nl/nieuws/belastingdienst-mag-bsn-niet-meer-gebruiken-btw-identificatienummer.

80 Cf. art. 16(1) Dutch General Data Protection Regulation Implementation Act in conjunction with art. 5:32(1) Dutch General Administrative Law Act and art. 58(6) GDPR.

Agency for violating the requirements set out in Article 32 of the GDPR with respect to its Employer Portal.[81] The Employee Insurance Agency has to be compliant by 31 October 2019.[82]

– The AP imposed, for the second time, an administrative enforcement order against the Dutch National Police for inadequate security of an IT system.[83] National Police has complied with the order.[84]

In 2019, the AP issued a €460,000 fine to a hospital in The Hague for insufficient internal security of patient records, in a case where dozens of hospital employees had had access to the medical records of a Dutch TV celebrity. The AP found that the hospital did not use two-factor authentication and failed in control of logging (article 32 GDPR). The hospital has announced that measures will be taken.[85]

Other violations found by the AP were stopped by other means such as informal enforcement action.[86] In 2018, the AP took informal action in 1,018 cases (298 data breaches and 720 complaints).[87]

Publication of sanctions

The AP has the power, based on the Dutch Freedom of Information Act[88] and in accordance with its publication policy guidelines, to publish, for instance, investigative findings and sanctions ordered against private companies or public authorities and other organisations, stating the name of the relevant organisation, even before a sanction has become final. The (primary) purpose is to inform and warn the public. Such publication by a supervisory

81 'AP dwingt UWV met sanctie gegevens beter te beveiligen', https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen.

82 'AP dwingt UWV met sanctie gegevens beter te beveiligen', https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen See also https://autoriteitpersoonsgegevens.nl/nl/nieuws/uwv-heeft-werkwijze-verzuimbeheer-aangepast-na-onderzoek-ap.

83 'Nationale Politie beschermt politiegegevens nog steeds niet goed genoeg', https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-beschermt-politiegegevens-nog-steeds-niet-goed-genoeg.

84 'Nationale Politie voldoet aan last onder dwangsom', https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-voldoet-aan-last-onder-dwangsom.

85 'Haga beboet voor onvoldoende interne beveiliging patiëntendossiers', https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers.

86 Annual Report 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf.

87 Ibid.

88 See i.a. Administrative Jurisdiction Division of the Council of State 31 May 2006, ECLI:NL:RVS:2006:AX6362, point 2.7 and Administrative Jurisdiction Division of the Council of State 10 November 2010, ECLI:NL:RVS:2010:BO3468, point 2.5.

authority is not to be considered as a sanction in itself[89], although this point of view is criticised in Dutch legal literature.[90]

Fining guidelines

On 14 March 2019, the AP published its new policy guidelines for calculating administrative fines.[91] In short, the AP divides infringements into several categories and assigns to each category a specific fine bandwidth and a 'basic fine' (the minimum of the bandwidth + 50% of the amount of the bandwidth). When calculating a fine, the AP will increase or decrease the amount of the basic fine depending on factors such as those referred to in article 83(2) GDPR. The previously mentioned fine imposed on the hospital is the first example of the application of the new fining guidelines.[92]

Question 12

Dutch law dictates that damages may consist of material loss or other disadvantages, though the latter only as far as the law implies that there is an entitlement to compensation. In that respect, by law the aggrieved party has a right of compensation for damages not consisting of material loss (such as injured honour or reputation) as well as a harmed memory of a deceased (provided that the deceased himself, if he would still be alive, could have claimed damages for injuring his honour or reputation).

In contradiction with compensation for material loss – which is in principle subject to full compensation – the extent of the compensation for intangible harm is assessed in conformity with the standards of reasonableness and fairness. Judges in the Netherlands have a discretionary power in assessing the extent of the compensation, meaning also that they may choose not to award any compensation at all.[93]

Notwithstanding the above, compensation for intangible damages is not easily awarded in the Netherlands, in any case not in large sums. In a court ruling where freedom of speech was juxtaposed with the freedom to privacy, compensation was awarded to an employee

89 See i.a. the Explanatory memorandum to the *Instellingswet ACM* (33 622), p. 57-58, Administrative Jurisdiction Division of the Council of State 2 August 2017, ECLI:NL:RVS:2017:2086, point 6.1 and District Court of Rotterdam 24 February 2017, ECLI:NL:RBROT:2017:5041, point 13.3. See also Court of First Instance 30 May 2006, Case T-198/03 (Lombard Club), ECLI:EU:T:2006:136 on the decision to publish the non-confidential version of a Commission decision.

90 See e.g., Handhavingsrecht (HSB) 2016/5.4.2.

91 'AP past boetebeleidsregels aan', https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan.

92 For that, see the EDPB Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

93 HR 27 April 2001, NJ 2002/91.

of a phone company whose name was repeatedly mentioned in a blog post by an angry journalist who had had a bad experience with the customer service, more specifically with the aforementioned employee.[94] The court ruled that the employee suffered from injured reputation, as it was easy to find the (disproportionate) allegations against her via search engines, putting her in a negative light and possibly making it difficult for her to find a new job. Even though the court refers to the injury of reputation as being "substantially", only € 500 was awarded.

Question 13

The Dutch Civil Code provides that a foundation or an association with full legal capacity can start legal proceedings aiming to protect similar interests of other persons, insofar as it is laid down in their statutes that they promote such interests.[95] In addition, the Awb provides for the possibility of the party / parties concerned to file an objection in an administrative procedure, whereby a party concerned may also be a legal person that protects general or collective interests following their stated purposes or factual activities.[96]

The UAVG provides though that a processing activity cannot be subject to legal proceedings under the Civil Code nor a formal objection in an administrative procedure under the Awb, if the person that is affected by the processing activity has objections against this.[97] This means that representative actions may only be initiated if the affected person(s) do not object. At the time of writing, no examples of such cases are until now available.

There are however several NGOs and initiatives in the Netherlands that play an important role with regard to pursuing the public interest in relation to privacy and the protection of personal data.

Bits of Freedom has, for example, developed a tool called "My Data Done Right". With this tool, over 17,000 people filed a request to get access to their data. Also, it organizes an annual and widely media-covered event giving a Big Brother award to the person or organization that has been deemed the biggest violator of privacy of that year.

Civil society has also campaigned for organizing a consultative referendum on the Dutch Intelligence and Security Services Act (In Dutch: *Wet informatie en veiligheidsdiensten*, hereinafter "Wiv"). Of the 6,7 million Dutch inhabitants that voted in

94 Rb. 's-Gravenhage 21 November 2007, KG 07/1158.

95 Art. 305a Civil Code - https://wetten.overheid.nl/BWBR0005291/2019-01-01/#Boek3_Titeldeel11_Artikel305a.

96 Art. 1:2 3rd indent Awb - https://wetten.overheid.nl/BWBR0005537/2019-04-02/#Hoofdstuk1_Titeldeel1.1_Artikel1:2.

97 Art. 37 UAVG.

this referendum, a majority voted against. Although the referendum was not binding, the government did adjust the Wiv to meet some of the worries of the public.

Question 14

In the national context, the AP cooperates with different other supervisory authorities and has signed cooperation agreements laying down the cooperation arrangements.[98] Usually a covenant is used to lay down how the supervisory authorities will cooperate and how they share the tasks and reach the goals that they have in common and for which they may cooperate. The AP has signed a covenant with the following organisations:

- The Dutch Media Authority (in Dutch: *Commissariaat voor de Media*)
- The Dutch central bank (in Dutch: *De Nederlandsche Bank*)
- The health and Youth Care Inspectorate in formation (in Dutch: I*nspectie Gezondheidszorg en Jeugd in oprichting (IHJ i.o.)) –*
- The Consumer and Market Authority (in Dutch: *Autoriteit Consument en Markt (ACM)*)
- The Dutch Healthcare Authority (in Dutch: *Nederlandse Zorgautoriteit*)
- The Inspectorate of Education (in Dutch: *Inspectie van het onderwijs*)
- The government service for identity data (in Dutch: *Rijksdienst voor Identiteitsgegevens*)
- Radiocommunications Agency (in Dutch: *Agentschap Telecom*)

Arguably, the cooperation between the ACM and the AP is the most relevant one with regard to the protection of personal data, as these two authorities have a shared responsibility concerning the use of personal data in relation to Dutch implementation of the ePrivacy Directive. The cooperation agreement mainly regulates the general exchange of information between the authorities and situations in which their competences overlap

Another covenant that warrants specific mention is the covenant between de AP and the DNB. Following the introduction of the Payment Services Directive 2[99], where third parties may get access to the banking details of a consumer after (s)he has given his / her consent, the AP and the DNB have entered into an agreement in which they demarcate their responsibilities towards the use of banking information.

In addition to bilateral agreements with the mentioned organizations, the AP also participates in the Markttoezichthoudersberaad, which is the meeting of regulators who (partly) focus on the functioning and behavior of market players. In addition to the AP,

98 https://www.autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/nationale-samenwerking.

99 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L337/35.

also the ACM, Financial Market Authority, The Dutch Media Authority, the DNB, the Netherlands Gambling Authority and the Dutch Healthcare Authority participate in the MTB.

There is no covenant or other agreement between de AP and the Dutch Ombudsman. However, where the Ombudsman deems the AP to be in a better position to help a citizen with a specific issue between the citizen and public authorities, he can refer a case to the AP. At the same time, the Ombudsman is able to hear and investigate complaints about the AP by citizens.

D Data Processing for National Security Purposes

Question 15

The Dutch Government has concluded that the processing of personal data for national security purposes as derogation from the regimes provided by the GDPR and the Law Enforcement Directive coincides with the processing of data as part of the work of the intelligence and security services.[100]

The UAVG "does not apply to the processing of personal data referred to in Article 2(2) of the GDPR."[101] However, by means of exception, it does apply, "to the processing of personal data […] in the course of an activity which falls outside the scope of Union law"[102]. However, the processing of personal data by or for the benefit of the Military Intelligence and Security Service and the General Intelligence and Security Service (in Dutch: *AIVD*) in relation to their tasks is again excluded.[103]

As a result, personal data processed by a private party but destined for use by one of the intelligence services does not fall within the scope of the UAVG nor the GDPR. However, the GDPR is applicable to the processing of personal data by other public bodies in the interest of national security, for example the processing as part of the performance of the tasks and competencies incumbent to the Minister of Justice in the interest of national security (for instance counterterrorism).[104]

100 EM UAVG, para. 2.2, www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

101 Section 2, para. 3, GDPR Implementation Act.

102 Section 3, para. h 1, sub a), and para. 2 GDPR Implementation Act. Art. 2(2) under a) of the Regulation is thus brought within the ambit of the Implementation Act and the GDPR.

103 EM UAVG, para. 2.2, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

104 Idem, see also H.R. Kranenborg and L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief*, Deventer, Kluwer 2018, p. 126.

The Wiv does not provide a detailed definition of the term 'national security'. It follows from the definition of the tasks of the AIVD that national security coincides with the maintenance of the democratic legal order, with security or with other important interests of the Dutch state.[105] Concerning the Military Intelligence and Security Service, the protection of national security requires mainly the maintenance of the international legal order and the readiness of the armed forces.[106]

The processing of personal data covered by the Wiv is broadly defined.[107] It encompasses data related to persons concerning whom there is a serious suspicion that they form a threat to the democratic legal order, to security or to other important interests of the Dutch state.[108] Data concerning enquiries or analyses related to other states and data related to persons who have been examined by foreign intelligence services fall under the Wiv as well.[109] Personal data necessary for the correct functioning of the services can also be processed under the Wiv, even as personal data needed to perform more general analyses of threats and risks.[110] Not only data concerning the persons directly related to these goals, but also to persons involved more indirectly can be collected when they form an inextricable part of a larger set of data.[111]

According to the AIVD the Wiv not only applies to names and addresses of its targets, but also data related to its suppliers and to applicants or persons or companies related to the service in any other way.[112] The AIVD indicates as well that certain categories of private companies, for instance providers of telecom services, have the legal obligation to provide data to the security services when required. They are not allowed to inform, amongst others, the person concerned of the transmission of these data.[113]

The laws implementing Directive (EU) 2016/680 do not define the terms 'national security' either. The Police Data Act provides for the transmission of personal data to the two aforementioned intelligence services for the purpose of the fulfillment of their tasks.[114] This possibility or obligation is contained as well in the Wiv.[115]

105 Section 8, para. 2, sub a) Intelligence and Security Services Act 2017.
106 Section 10, para. 2, sub a), ibid.
107 Section 19, para. 1, 2 and 5, ibid.
108 Section 19, para. 1, sub a), ibid.
109 Section 19, para. 1, sub c) and d), ibid.
110 Section 19, para. 1, sub e) and g), ibid.
111 Section 19, para. 5, ibid.
112 www.aivd.nl/onderwerpen/aivd-en-privacy/documenten/publicaties/2018/05/25/naar-aanleiding-van-bescherming-van-persoonsgegevens-met-de-avg.
113 Ibid.
114 Section 24 Police Data Act.
115 Sections 91-94 Intelligence and Security Services Act 2017. This obligation to cooperate with the security and intelligence services, also exists for the military police, the tax authorities, the social security services and the immigration office. Section 93 provides for the transmission of data by the Prosecutors office.

Application of the EU Charter of Fundamental Rights

According to the Explanatory Note to the Wiv, the acts of the intelligence and security services fall, pursuant to article 4, paragraph 2, TEU, outside the scope of the powers of the Union. Hence, the processing and retention of personal data by these services do not fall under the EU privacy legislation. The Charter is only applicable to the implementation of EU law by the Member States.[116] The privacy rights of the constitution and the ECHR are however applicable.

The Council of State considered in this respect that EU law and the case law from the Court of Justice do not apply to the intelligence and security services. However, it is likely that the principles developed by the ECJ are relevant for the scope and limitation of their powers.[117]

116 E.M. Intelligence and Security Services Act 2017, p. 250, www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten.

117 Opinion from the Council of State regarding the draft Intelligence and Security Services Act 2017 and explanatory memorandum www.raadvanstate.nl/@64162/w04-16-0097/.

Norway

Milos Novovic and Martin Hennig[*]

A Setting the Scene

Question 1

In Norway, the General Data Protection Regulation (hereinafter "GDPR") has been implemented through the Norwegian Personal Data Protection Act ("PDPA", Lov om behandling av personopplysninger (*personopplysningsloven*), LOV-2018-06-15-38). The PDPA is a relatively concise law, which, in addition to implementing GDPR, introduces several provisions aimed at supplementing GDPR requirements, or making use of flexibilities offered under the GDPR.

Of special interest is chapter 3 of the law, which is specifically geared towards introducing supplementary provisions into the national law.

Article 5 deals with the question of the consent of children to personal data processing, and sets the age of consent to 13 years, in line with art. 8(1) of the GDPR.

Article 6 deals with use of special categories of data in employment relationships, and prescribes that such data processing is lawful insofar as it is necessary in order to fulfil rights and duties under employment law.

Article 7 establishes the possibility for the Norwegian Data Protection Authority to authorize processing of special categories of personal data, where such processing is in the public interest. In Article 8, the possibility to process personal data for research, archival or historic purposes is retained, provided that safeguards mentioned in article 89(1) of the GDPR are implemented.

Article 11 stipulates that comprehensive criminal records shall only be processed by public authorities, and Article 12 stipulates that national ID numbers are to be used only where there is an actual need for secure identification, and their use is needed for such identification. Several provisions point to the possibility of future administrative acts stipulating the use of data in further detail.

* Milos Novovic: Associate Professor, Department of Law and Governance, BI Norwegian Business School. Martin Hennig: Associate Professor, Faculty of Law, UiT, The Arctic University of Norway.

Furthermore, Chapter 4 deals with exceptions to data subject rights. Article 16 details exceptions to the right of information and right of access, whereas Article 17 details the exceptions applicable in cases where personal data is being processed for research purposes.

According to article 17, a data subject's right to information and access can be limited in cases where information:

a. is of importance to Norway's foreign policy interests or national defense and security interests, when the controller can exempt the information pursuant to the Norwegian Freedom of Information Act;
b. it must be kept secret for the purposes of prevention, investigation and legal prosecution of criminal offenses
c. it must be considered unreasonable for the data subject to become aware of information in order to safeguard his or her health or the relationship with persons close to him or her;
d. is subject to the duty of confidentiality in law or pursuant to law;
e. is only found in texts prepared for internal case preparation, and which have not been disclosed to others, insofar as it is necessary to refuse access to ensure sound internal decision-making processes
f. it would be contrary to obvious and fundamental private or public interests to disclose information.

Articles 20 and 22 establish the work of supervisory authorities, and detail the scope of their tasks. The Norwegian Data Protection Authority (*Datatilsynet*) has the general responsibility for oversight of the implementation of PDPA, whereas The Privacy Appeals Board, (*Personvernnemnda*), acts as a second-instance administrative authority in individual cases.

Question 2

There is no explicit distinction between these rights, although in the context of private parties, violation of someone's right to private life is also retained as a tort under the Norwegian Tort Act (*Skadeerstatningsloven*). There is no case law clearly outlining the scope of either one of these rights, or elaborating on the differences between violation of the right to data protection versus the right to private life.

In this regard, it should be mentioned that the EU Charter of Fundamental Rights (hereinafter "Charter") is not part of the EEA Agreement, and is thus, at least formally speaking, not binding upon Norwegian authorities. However, The EFTA Court has long

held that the EEA Agreement must be 'interpreted in the light of fundamental rights.'[1] Thus, the influence of the case law from the European Courts concerning the Charter and data protection will undoubtedly be monitored closely by Norwegian courts and public authorities.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The Norwegian National Supervisory Authority (hereinafter "NSA") has issued several guidelines which deal with these topics and has made a reference to these principles, although without going into much depth. While there is no new case law as of date, the courts have ruled in a few cases under the law implementing the Directive.

NSA-issued Guidelines on "basic privacy principles" explain these concepts, but are quite short and superficial. They do not offer any in-depth coverage of examples, and do not offer any insights into enforcement practice.

The court cases dealing with implementation of the Directive have focused on the purpose limitation principle when assessing whether processing qualified as compatible further processing. The most famous case made its way to the Supreme Court (HR-2013-234-A). A driver who had been dismissed because of discrepancies between his time sheets and the electronic (GPS) log of his vehicle, requested damages for non-economic loss under section 49 subsection 3 of the Personal Data Act. The Supreme Court's majority concluded that reusing information collected for a different purpose than the original one cannot be anchored directly in Section 8(f) of the Personal Data Act (legitimate interest). The conditions in Section 11(1)(c) (purpose limitation) must also be satisfied. In the specific case, the employer's comparison of the log and the time sheets represented a reuse that had no basis in Section 11(1)(c), as the purposes were not compatible. This led to the Court declaring the processing unlawful, even though the legitimate interest test was apparently satisfied. It should be noted that the case was decided under the old law, implementing the Directive.

1 See for example the judgment of 28 September 2012 in Case E-18/11 *Irish Bank* [2012] EFTA Ct. Rep. 592, para. 63.

Question 4

There is limited case law on interpretation of these topics, both under the Directive and under GDPR. The Norwegian Supreme Court has not examined the validity of consent in individual cases, and remarks on legitimate interest have been quite sporadic, and mostly limited to the aforementioned case LOD-2013-114-24. In the case "legelisten.no", decided by Oslo District Court, 17 December 2019, the court found that the performance assessment of individual medical doctors (general practitioners) provided by "legelisten.no", was compatible with article 6 of the GDPR. The case concerned the processing of evaluations by patients of their experience with individually named medical practitioners in Norway. The Norwegian Medical Association argued that the processing of information about the general practitioners constituted personal data that required protection under article 6(1)(f). The District Court disagreed, and ruled that the legitimate interest of "legelisten.no" in publishing their experience with general practitioners was protected by freedom of speech and outweighed the need for the protection of the practitioners' personal data.[2]

Question 5

Such debate has largely been absent, although several research projects are currently exploring data commodification as a topic. Some criticism has been issued against the European Data Protection Board's (hereinafter "EDPB")Draft Guidelines on article 6(1)(b) GDPR which take a firm stance against use of personal data as a contractual counter-performance, suggesting the need to balance the right to data protection with the right to freedom of contract. As Novovic surmised, criticizing the EDPB's statement on the fact that personal data cannot be a contractual counter-performance, exceeds the scope of authority of the EDPB and goes beyond questions of the GDPR:

"Contract interpretation – and contractual validity – is clearly and firmly within the domain of *national courts* to decide under the governing law. By making sweeping statements on the "general purpose of the contract" for the entire categories of online services,[3] and consequently engaging in contract interpretation, the EDPB is seriously *overstepping its authority* and the scope of tasks conferred on it by the virtue of article 70 of the GDPR.

2 See the judgment of 17 December 2019, Oslo District Court, TOSLO-2019-98312. As of 18 February 2020, it is not known whether or not this case has been appealed by the Norwegian Medical Association.

3 See, for example, Guidelines, para. 50: "Further to this, Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. *Although such processing may support the delivery of a service, it is separate from the objective purpose of the contract between the user and the service provider, and therefore not necessary for the performance of the contract at issue.*" Emphasis added.

This becomes even more problematic when, in the context of discussing a particular type of online service, EDPB states that "*personal data cannot be a tradeable commodity*", and underlines that that "data subjects can agree to processing of their personal data, *but cannot trade away their fundamental rights"*.

There are at least three issues with placing such statement in this context.

First, there is still a deep scholarly discussion on the commodification of personal data, and the GDPR itself does not address the issue directly. Such strong statements on the issue are best left to the legislative branch, or alternatively, the judiciary – as it is questionable how the EDPB reaches such sweeping conclusion in the Guidelines, and from where it derives authority to do so.

Secondly, implying that entry into a certain *type* of a contract would, in itself, entail "trading away fundamental rights" has no basis in the law. Once again, this assessment would need to be made on a *case by case basis*, with a full due reference to national contract laws, and careful balancing of different rights.

Thirdly, the EDPB seems to surprisingly ignore the fact that freedom of contract is *also* seen as one of the fundamental rights within EU, falling under the scope of the Charter of Fundamental Rights of EU. *This discussion should have been given a central place in the Guidelines*; as pointed out by various authors, the jurisprudence of the Court of Justice of the European Union (hereinafter "CJEU") on the topic extends to the topics such as freedom to enter into a contract, freedom from contract, freedom to choose a contractual partner, and freedom to determine the content of a contract. Additionally, the CJEU has on multiple occasions clearly stated that EU instruments cannot be implemented or interpreted in a way which would jeopardize protection of *other* fundamental rights:

> "It must be borne in mind, in the first place, that, according to the case-law of the Court, EU law requires that, when transposing directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the EU legal order. Subsequently, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of EU law."[4]

4 Judgement of 16 July 2015 in Case C-580/13, *Coty Germany v Stadtsparkasse Magdeburg*, ECLI:EU:C:2015:485.

In other words, the data subject's right of data protection would need to be *balanced* against the right of freedom of contract on an *individual* basis. It is outside the purview of EDPBs authority to prioritize one fundamental right over another in a generalized manner, and the Guidelines should be consequently amended."[5]

Question 6

No such acts have been introduced as of yet, although there have been some discussions on the scope of this right in the proposal for the new Public Administration Act (Norway).[6] Whether such measures will be introduced remains to be seen.

In the comments to the proposed Public Administration Act, the Law Commission is aware of and adresses the imminent challenges presented by automated decision-making. As regards this issue, the Law Commission states that (English summary):[7]

> "The draft act facilitates further digitalisation of administrative activities. The individual provisions are in principle intended to be technology-neutral. The draft act envisages that administrative proceedings may be fully automated following detailed assessment of relevant areas, subject to a requirement that the legal content of the system must be publicly documented. The Commission has also examined particular challenges presented by digitalisation and automation in the data protection context. These raise difficult issues both nationally and under international law; see particularly the EU General Data Protection Regulation (GDPR). The Commission is proposing an expanded power for administrative bodies in the central government, county and municipal sectors to share confidential information. In the case of personal data, it is proposed that this power be granted subject to conditions that satisfy GDPR requirements."

5 Milos Novovic, Answer to the Public Consultation of the EDPB on Guidelines on Article 6(1)b in the context of online services.

6 See NOU 2019: 5, "Ny forvaltningslov — Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven)", published by the Ministry of Justice and Public Security, see https://www.regjeringen.no/no/dokumenter/nou-2019-5/id2632006/. All webpages referred to were visited 18 February 2020.

7 See NOU 2019: 5, "Ny forvaltningslov — Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven)", published by the Ministry of Justice and Public Security, Summary in English, 2.2.2 General comments on the Commission's proposals, https://www.regjeringen.no/no/dokumenter/nou-2019-5/id2632006/?ch=3.

Question 7

Case law on the application of the right to erasure is very sparse. Most court cases and enforcement actions were connected with employers' failure to erase employees' email accounts. However, instead of referring to the right of erasure, the courts referred to specific provisions found in the bylaw implementing PDPA, and found employers in the violation of this specific provision.

Question 8

No such law has been introduced to date.

C Domestic Enforcement of Data Protection Law

Question 9

Although no single Norwegian public authority has been charged with the responsibility of enforcing the rights and obligations laid down in the GDPR, it is the Norwegian Data Protection Authority which has been entrusted under the Norwegian Personal Data Protection Act (hereinafter "PDPA") to enforce the GDPR. The Norwegian Data Protection Authority handles complaints as the first instance, and the Privacy Appeals Board is the appellate administrative body. The procedures relating to supervision and complaints regarding the enforcement of the GDPR are found in Chapter 6 of the PDPA.

As of today, there is little "enforcement record" to speak of. However, in March 2019, the Norwegian Data Protection Authority imposed an administrative fine of 1.6 million Norwegian kroner, or the equivalent of €170,000, on the Municipality of Bergen. The fine stems from inadequate security measures in place for the protection of usernames and passwords belonging to over 35,000 user accounts in the municipality's computer system. Due to insufficient security measures, these files had been left unprotected and openly accessible. The Municipality of Bergen later stated that it did not wish to appeal the decision.[8]

8 See the Report by The Norwegian Data Protection Authority (*Datatilsynet*), published 12 April 2019, https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/administrative-fine-of-170,000--imposed-on-bergen-municipality/.

Question 10

The Norwegian NSA has taken a few high-profile cases, most of which were tied to data protection practices in the public sector (education and healthcare). Almost all enforcement actions stemmed from breaches of article 32 of the GDPR, so there is a clear focus on data security as an enforcement mechanism trigger. This might be a flawed strategy long-term, seeing as it might encourage a rather narrow reading of data protection obligations by data controllers.

Aside from prioritizing highly publicized cases, the NSA seems to be discouraging data subjects from submitting complaints. The website instructs data subjects to submit written complaints, claiming that electronic submission forms are not ready for public use due to security concerns. The website also urges data subjects to resolve their issues directly with data controllers.

Question 11

We are not aware of such sanctions being imposed at this point.

Question 12

The Norwegian legal system does make it possible to claim damages for intangible harm (*oppreisning*). The PDPA makes this explicitly possible in cases of harm suffered as a consequence of its breach.

Calculation of damages is discretionary and depends on the nature and scope of violation, as well as severity of consequences. Traditionally, very low monetary amounts have been awarded in data protection cases, with the highest amount being around €5,000.

Question 13

There are no such movements in Norway as of date, to the best of our knowledge.

Question 14

To the best of our knowledge, our national NSA, the Norwegian Data Protection Authority does not cooperate, or at least not formally, with other regulators or the Norwegian Ombudsman. However, cooperation with other public authorities is not inconceivable, for instance in the case of collaboration on specific projects.

D Data Processing for National Security Purposes

Question 15

So far, Norwegian regulatory authorities have not made any attempt in national legislation at defining, or in any way restricting, what constitutes "national security" under article 23(a) of the GDPR. It is worth noting, that in the Norwegian Personal Data Protection Act, article 23(3) states that the processing of personal information which is necessary from the point of view of safeguarding national security, is completely excluded from the GDPR. This provision also states that personal information relating to the security of our allies, foreign states or relating to other vital national security interests, are excluded from the GDPR.

In comparison to the text of the GDPR, at least at first glance, the Norwegian Personal Data Protection act seems to have a wider scope of exception than article 23 of the GDPR. Especially in regards to the possibility of excluding personal information relating to our allies, the scope of the exception seems wider under the Norwegian act than in the GDRP. However, it would be remarkable if the GDPR would block the exclusion of information, which Norwegian authorities considered sensitive to our allied countries. Time will show if this question of interpretation of the scope of the exception arises in the future.

Poland

Agnieszka Grzelak and Mirosław Wróblewski[*]

A Setting the Scene

Question 1

The main legal instruments adopted in order to implement the General Data Protection Regulation (hereinafter "GDPR")[1] in Poland are as follows:

1. the Act of 10 May 2018 on personal data protection[2] (PDPA), which repealed the Act of 29 August 1997 on personal data protection (hereinafter "PDPA97");[3]
2. the Act of 21 February 2019 amending some acts as regards ensuring the application of GDPR (hereinafter "GDPRImpl").[4]

Moreover, on 14 December 2018 the Polish Parliament adopted the Act on personal data protection processed with regard to the prevention and fight against crime[5] (hereinafter "PDPACrime"), implementing the Directive 2016/680[6].

PDPA specifies, among others, general conditions for imposing administrative fines, a new DPA – data protection authority (the President of the Office for the Protection of Personal Data – PUODO), public entities obliged to appoint a Data Protection Officer, the administrative procedure pertaining to the personal data breach procedure, civil and criminal liability for breaches of personal data protection legislation. This is also the Act in which the Polish legislator decided to introduce some derogations from GDPR, however,

---

* Agnieszka Grzelak: Professor of European and International Law at Kozminski University, Warsaw, Poland; Mirosław Wróblewski: Attorney at law, Director of Constitutional, International and European Law Department in the Office of the Commissioner for Human Rights, Warsaw, Poland.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Journal of Laws (JL) 2018, item 1000 as amended.

3 JL 1997, No 133 item 883 as amended; PDPA in English, www.uodo.gov.pl/en/594. All webpages referred to were visited on 15 January 2020.

4 JL 2019 item 730.

5 JL 2019 item 125.

6 Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L119/89.

flexibilities of GDPR were availed by the Polish legislator only to some extent. This can be illustrated by the following examples. Articles 3 and 4 PDPA avail generally of the flexibility of article 23 GDPR, limiting information obligations foreseen by articles 13 and 14 GDPR with regard to controllers being a public authority. The ability to take advantage of this possibility depends on compliance with the following conditions: 1) changing the purpose of processing is used to implement a public task; 2) failure to comply with the information obligation is necessary to achieve the objectives referred to in article 23 GDPR; 3) providing information required by article 13(3) GDPR: a) prevents or significantly hinders the proper performance of a public task, the interest or fundamental rights or freedoms of the data subject are not superior to the interest arising from the implementation of this task public, or b) violates the protection of classified information. Article 5 PDPA, which limits the application of Article 15(1-3) GDPR is constructed in a similar way.

GDPRImpl amended other sectoral acts allowing for even further limitations of GDPR norms. For example, laws regulating legal professions (Act on advocates and Act on attorneys at law[7]) limit application of GDPR (especially articles 15, 18, 19 and 21) to the scope not infringing professional secrecy. Those laws also avail of the possibility foreseen by article 90 GDPR – competences of the DPA do not prevail over the duty to keep professional secrecy.[8]

As regards article 6(1)(c) GDPR, GDPRImpl amended sectoral acts, in order to – among others – secure the legality of data processing. GDPRImpl therefore amended i.a. Code of administrative procedure,[9] Labour Code,[10] Act on public roads,[11] Act on fisheries[12] and more than 160 others sectoral laws, in cases necessary for compliance with a legal obligation to which the controller is a subject.

As for articles 86-90 GDPR, it should be stated that the legislator has not taken any special actions to amend any provisions regarding the access to public information or the national personal identification number (PESEL), which were in force already before 2018. In turn, in relation to the processing of personal data in employment, the legislator has originally decided on the preservation of provisions of the Labour Code being previously in force (art. 22^1§ 1) and on adding new rules on the admissibility of the application of visual surveillance and other forms of monitoring employee at work. Later on (in February 2019) the Parliament modified the Labour Code by changing the scope of data that an employer may request from an employee in connection with employment. For example,

7 The Act of 26 May 1982 (JL 2018 item 1184 as amended) and the Act of 6 July 1982 (JL 2018 item 2115 as amended).
8 See e.g. art. 5b of the Act on attorneys at law.
9 The Act of 14 June 1960 (JL 2018 item 2096 as amended).
10 The Act of 26 June 1974 (JL 2019 item 2046).
11 The Act of 21 March 1985 (JL 2017 item 2222 as amended).
12 The Act of 18 April 1985 (JL 2018 item 1486 as amended).

since 4 May 2019 the employer may not request the job applicant to provide parents' names and place of residence (correspondence address). However, the employer is entitled to request contact details from the applicant (e.g. telephone number, e-mail address). Another example illustrates the way in which the legislator introduced derogations from article 89 GDPR in relation to academic activities. In article 2(2) PDPA it was decided that with regard to the academic activity, the provisions of articles 13, 15(3) and (4), 18, 27, 28(2-10) and article 30 GDPR do not apply.

On the other hand, article 8 GDPR allows to reduce the age limit from 16 to 13 of a child whose data is processed in the context of information society services. Although this was the subject of a public debate, ultimately the Polish legislator decided not to use this option and to remain the 16 years limit. Interestingly, the same age is applied in Poland as a threshold for independent decision making capacity as regards medical services.[13]

Question 2

The Constitution of Poland distinguishes between right to privacy and right to protection of personal data. According to article 47 of the Constitution (hereinafter "Const"), everyone shall have the right to legal protection of private and family life, of honour and good reputation and to make decisions about personal life. This provision reflects article 7 of the Charter of Fundamental Rights of the EU (hereinafter "Charter") and article 8 of the European Convention on Human Rights (hereinafter "ECHR"). However, the protection of freedom and privacy of communication is safeguarded by a separate provision (article 49 Const).

The constitutional protection of personal data, being a specific emanation of right to privacy, is much more detailed. Article 51 Const explicitly establishes specific requirements securing informational autonomy of an individual: 1. No one may be obliged, except on the basis of statute, to disclose information concerning his person; 2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law; 3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute; 4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute; 5. Principles and procedures for collection of and access to information shall be specified by statute. Constitutional protection is thus far-fetched, in a manner similar

13 The constitutionality of those rules were confirmed in the CC judgment of 11 October 2011 in Case K 16/10, http://trybunal.gov.pl/sprawy-w-trybunale/art/1567-wyrazenie-zgody-na-leczenie-przez-osobe-maloletnia.

to the requirements arising from article 8 Charter (with the exception regarding Charter's institutional requirements).[14]

Public authorities are obliged to prevent violations of privacy, since the protection by both civil and penal law is a *post factum* protection, thus cannot be treated as sufficient. The right to privacy is guaranteed by civil law (protection of personal goods – articles 23 and 24 Civil Code[15]) and by penal law (e.g. prohibition of defamation – article 212 Penal Code[16]). Only on the basis of the Code of Civil Procedure (CCP, article 755)[17] any interim measure regarding privacy can be established by a court.

Data protection is based mostly on the administrative law system, including institutional protection by DPA. However, civil and penal law mechanisms may also be used, as it is clearly provided by PDPA and GDPR. A set of legal measures and sanctions is broader and more diversified in comparison with the protection of privacy.

The rights to privacy and data protection, as set out in the Charter, have influenced the interpretation of the Polish law only to a certain extent. This is most evident in the case law of the Constitutional Court (CC). For example, the Court of Justice of the European Union (hereinafter "CJEU") judgment in *Digital Rights Ireland* Case,[18] in which articles 7 and 8 Charter were interpreted, influenced the judgment of CC in the surveillance case.[19] Recently, the concept of independence of an authority referred to in article 8(3) Charter, together with the relevant case law of CJEU[20], was the subject of discussions during the work on provisions regulating the systemic aspects of functioning of the DPA.[21]

14 See M. Wild, 'Komentarz do art. 47', in M. Safjan & L. Bosek (Eds), *Konstytucja Rzeczypospolitej Polskiej Vol. I, Komentarz do artykułów 1-86*, Warszawa, C.H.Beck, 2016, pp. 1161-1182.

15 The Act of 23 April 1964 (JL 2019 item 1145).

16 The Act of 6 June 1997 (JL 2018 item 1600 as amended).

17 The Act of 17 November 1964 (JL 2018 item 1360 as amended).

18 Judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Digital Rights Ireland), ECLI:EU:C:2014:238.

19 Judgment of CC of 30 July 2014 in case K 23/11, OTK-A 2014, No 7, item 80.

20 See for example judgment of 8 April 2014 in Case C-288/12, *European Commission v. Hungary,* ECLI:EU:C:2014:237.

21 A. Grzelak & M. Wróblewski, 'Niezależność Prezesa Urzędu Ochrony Danych Osobowych w świetle prawa UE', in M. Gumularz et al. (Eds), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa, MustRead-Media Ed., 2018, p. 219.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

On the basis of GDPR, neither DPA nor Polish courts interpreted these basic data protection principles in a way that could be subject to reporting here. However, in the first case in which the financial penalty was imposed by DPA on the company, the administrative court of first instance analysed the legitimacy of the penalty and shared DPA's statement that the infringement is of a serious nature, as it also violates the principle of transparency and fairness[22]. Therefore, the information can be given on the basis of the previous legislation, with an indication that it may also be applied accordingly to the basis of new provisions.

PDPA97, which implemented Directive 1995/46/EC,[23] did not mention specifically the 'fairness' principle. Although the Polish text of article 6(1)(a) Directive 1995/46/EC explicitly used this term, PDPA97 in article 26 stipulated 'due diligence' as a controller's duty. Such a difference was interpreted in the literature either as a proper implementation of Directive 1995/46/EC or as a deviation from the EU legislation – the latter meant that PDPA97 missed the fairness principle, concentrating only on lawfulness. On the other hand, one may also say that in practice the duty of 'due diligence' in processing data served as a synonym of 'fairness'.[24] The administrative courts' case law followed such interpretation, e.g. the Supreme Administrative Court (SAC) emphasized that no organizational or financial reasons can justify unfair and illegal processing of personal data by banks.[25] That means, that in practice also the Polish DPA used concepts of 'due diligence' and 'fairness' in assessing the processing of personal data on the basis of PDPA97.[26] At the moment, GDPR leaves no room for such discussion anymore, however the concept of 'fairness' is broad. Currently, in the doctrine it is interpreted as a demand to find a proportionate balance between the interests of data subjects and controllers.[27]

The principle of purpose limitation was implemented already in article 26(1)(2) PDPA97. PDPA97 protected i.a. the execution of a controller's information duties and

22 This topic of fairness was not further explored. Cf. judgment of 11 December 2019 in Case II SA/Wa 1030/19, orzeczenia.nsa.gov.pl/doc/30EDD316DA.

23 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

24 P. Barta & P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa, C.H.Beck, 2015, p. 288.

25 Judgement of 4 March 2002 in case II SA 3144/01, Monitor Prawniczy 2002, No 8, p. 340.

26 Annual reports of DPA until 2018 are available on the webpage: giodo.gov.pl.

27 E. Bielak-Jomaa & D. Lubasz (Eds), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa, Wolters Kluwer, 2018, p. 327.

introduced the principle that data collected for a specified purpose cannot be used otherwise. The latter principle shall be understood as a prohibition of data processing for a purpose which is incompatible with the original purpose.[28] GDPR introduces no further changes in the understanding of this principle.

The principle of data minimisation was also present in PDPA97, in the concept of 'adequacy' of data processing (article 26(1)(3) PDPA97). According to the decisions of the Polish DPA, data was adequate when the processing was 'necessary'.[29] Data processed by a controller had to be necessary to achieve a purpose of processing; the scope of the data processed could not be broader. This line is confirmed in DPA's decision on the grounds of GDPR.[30] Adequacy of data was also protected both in well-established administrative courts' case law,[31] as well as in the judgments of CC, which interpreted article 51(2) Const and emphasized that public authorities cannot collect all useful, but only necessary data.[32]

Question 4

On the basis of PDPA97, administrative courts acknowledged that each legal basis of data processing, enumerated in article 23 PDPA97, had an autonomous and independent character, thus they had been granted, as a rule, the equal status.[33] This case law remains applicable also as regards the legal basis enlisted in article 6(1) GDPR.[34]

The previous case law regarding the consent – as a legal basis of data processing – also seems to be up-to-date and useful in interpretation of article 6(1)(a) and article 7 GDPR. According to the judgments, both the consent as well as all aspects of it must be clear in the moment the consent is given.[35] The consent thus shall be informed.[36]

As regards digital environment one shall mention disputable DPA's decisions concerning the consent given via electronic means of communication (mail, Internet forms). The DPA decided that within one's will only one consent can be given at one time, therefore a data subject cannot give in a single action a consent to process data and to make them available

28 P. Barta & P Litwiński, 2015, p. 294.

29 Ibid, p. 297.

30 E.g. DPA's address to Minister of Finance of 12 February 2019 (case ZSPU.023.38.2019.EKR) concerning data processing of coal's consumers, https://uodo.gov.pl/pl/file/1951.

31 P. Barta & P. Litwiński, 2015, p. 298.

32 Judgment of 21 November 1995 in case K 12/95, OTK 1995, No 2, p. 132.

33 Judgment of the Regional Administrative Court (RAC) in Warsaw of 1 December 2005 in case II SA/Wa 917/05; judgment of RAC in Warsaw of 31 March 2006 in case II SA/Wa 2395/04.

34 P. Litwiński et al, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*, Warszawa, C.H.Beck, 2018, p. 276.

35 Judgment of SAC of 4 April 2003 in case II SA 2135/02, Wokanda 2004, No 6, p. 30.

36 M. Jagielski, 'Pojęcie świadomej zgody w naukach prawnych', in K. Łakomiec & M. Wróblewski (Eds), *Realizacja zasady informed consent w kontekście realizacji lekarz*-pacjent: wyzwania i bariery rozwojowe w Polsce, Warsaw 2012, p. 21.

at the same time, because of different purposes (one consent based on the Act of electronic services,[37] second consent based on data protection legislation). Such interpretation of digital consent has been criticized from the perspective of electronic telemarketing realizing in practice one and the same economic purpose.[38] It is however to be noted that the DPA's position was upheld by the judiciary.[39]

As for the legitimate interest, article 23(4) PDPA97 pointed out two examples: direct marketing of the controller's own products and services, as well as pursuing claims for business activity. It seems that the cases referred to in this provision may still be considered as a legitimate interest based on Article 6(1)(f) GDPR. There have been doubts whether the legitimate interest basis (article 6(1)(f) GDPR) calls for the controller's interest to be based on specific provisions of law.[40] However, these doubts are to be rejected since the legitimate interest basis is not aimed at public authorities, it would also limit the scope of application of article 6(1)(f) GDPR and would compromise the purposes of GDPR. Therefore the interpretation of a legitimate interest basis shall be broad, covering economic, factual and legal interest of a controller.[41]

Question 5

The debate as regards the validity of personal data as 'counter-performance' for the provision of digital content has been very limited in Poland. Those problems were analyzed only by some civil society organizations, like the "Panoptykon" Foundation (dealing with fundamental rights and freedoms in the context of fast-changing technologies and growing surveillance), e.g. in the report "Tracking and profiling in the net. How from being a client you become a commodity",[42] and by academia.[43] Recently the problem of handling of data was shortly discussed in the media in the context of the FaceApp application, which was suspected of violating privacy principles. Eventually the Minister of Digitization took action demanding from institutions subordinated to him (CERT, NASK) to analyze safety from a technical angle, but also addressing PUODO. In his letter, the Minister drew attention to, among other things, the need for such applications to ensure their compliance with the provisions of GDPR, which requires that all information and all communications

37 The Act of 18 July 2002 (JL 2019 item 123).

38 P. Barta & P. Litwiński, 2015, p. 227.

39 The administrative court judgement of 19 November 2001 in case II 2748/00, www.giodo.gov.pl/data/filemanager_pl/110.pdf.

40 P. Barta & P. Litwiński, 2015, p. 222.

41 W. Chomiczewski, 'Komentarz do art. 23', in E. Bielak-Jomaa & D. Lubasz (Eds), 2018, p. 391.

42 K. Szymielewicz, K. Iwańska, 'Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem', January 2019, panoptykon.org/biblio/sledzenie-i-profilowanie-w-sieci-jak-z-klienta-stajesz-sie-towarem.

43 A. Mednis, Prawo ochrony danych osobowych wobec profilowania osób fizycznych, Warszawa, PressCom, 2019, p. 240.

related to the processing of personal data should be easily accessible and understandable, and formulated in clear and simple language.[44]

Of course also in Poland, following the Facebook-Cambridge Analytica scandal, there has been some public interest and debate regarding the processing of data by technology giants. On 30 March 2018, the Ombudsman (hereinafter "RPO") sent the general letter to the General Inspector of Data Protection (GIODO – DPA until 2018)[45] in which he addressed that problem as well, recognizing the Cambridge Analytica problem as a threat not only to the right to privacy of the internet user, but also for broadly understood democratic processes and protection of other rights of citizens. GIODO has not answered at all.

Question 6

GDPRImpl introduced many amendments in legislation to ensure that the right of not being subject to automated decision-making does not apply in certain situations. One may point at:

- article 105a Banking Law,[46]
- article 55a Road Transport Law,[47]
- article 98d and 136c Act on Obligatory Insurance, Insurance Guarantee Fund and Polish Motor Insurers' Bureau,[48]
- article 41 Insurance and Reinsurance Activities Law,[49]
- article 47c National Tax Administration Law,[50]
- separately – Tax Ordinance was amended (article 119zn § 2).[51]

As regards measures to safeguard the rights, freedoms and legitimate interests of data subjects, they were incorporated in above enlisted amendments, or already existing legal measures were deemed to be sufficient. These regulations provide i.a. for a right of a natural person to question decisions made in automated decision-making procedures, a right to express one's opinion in the matter and a right to appeal to a human being. The controllers using profiling were obliged to explain the basis of decisions made out of a profiling. The

44 Ministerstwo Cyfryzacji, 'Bezpieczeństwo aplikacji mobilnych: akcja – reakcja', www.gov.pl/web/cyfryzacja/bezpieczenstwo-aplikacji-mobilnych-akcja-reakcja.

45 RPO, 'Pismo RPO do GIODO w sprawie Cambridge Analytica', www.rpo.gov.pl/sites/default/files/Pismo%20RPO%20do%20GIODO%20w%20sprawie%20Cambridge%20Analytica.pdf.

46 The Act of 31 January 1989 (JL 1992 No. 72 item 359 as amended).

47 The Act of 6 September 2001 (JL 2019 item 58 as amended).

48 The Act of 22 May 2003 (JL 2018 item 473 as amended).

49 The Act of 11 September 2015 (JL 2019 item 381 as amended).

50 The Act of 16 November 2016 (JL 2018 item 508 as amended).

51 The Act of 29 August 1997 (JL 2019 item 900 as amended).

legal measures specify exhaustive categories of personal data, which can be used in automated decision-making. Thus other data cannot be used by a controller. Such legal measures were included, i.a. in the Banking Law and in the Insurance and Reinsurance Activities Law, to secure individual rights in profiling processes aimed at analyzing credit or insurance risks.

Question 7

The right to erasure established by Directive 1995/46/EC was implemented in article 32(1)(6) PDPA1997. According to this provision, every person had a right to ask for data erasure only when they were incomplete, not updated, inaccurate, collected illegally or no longer necessary in relation to the purposes for which they were collected. This provision has been rather consistently applied by DPA. However, there have been some divergences in the administrative courts' case law. One of the most prominent examples is the case of the withdrawal from the Catholic Church (apostasy), where the issue of personal data erasure of apostates arose. RPO pointed at three different lines of case law as regards that problem.[52] As a result, SAC decided that DPA is not entitled to control internal regulations of the Catholic Church, and the sole document confirming apostasy may only be a transcript of a baptism certificate with an apostasy annotation.[53]

The right to erasure may be realized in practice by decisions of DPA or in procedures of the protection of personal goods before civil courts. One shall pay attention to the Supreme Court (SC) judgment referring to the right to be forgotten within such a procedure.[54] A telephone conversation of a policeman with an elderly woman was made public on the internet – in fact such a publication lampooned her, since she had difficulties in communication. The SC confirmed that a data subject in such a situation is entitled to ask the controller to take reasonable steps to inform those controllers, who are processing the personal data, that the data subject has requested the erasure by such controllers of any links to, or copies or replications of, those personal data. One may however point at the SC's requirement that the judgment, acknowledging such a right, must be unequivocal and cannot give any room for interpretation by the parties.[55]

The problem of the right to erasure, however not particularly in the context of search engines, but with relation to the right of information, also arose in an earlier legal situation

52 RPO, 'Motion of 19 October 2017', www.rpo.gov.pl/sites/default/files/Wniosek%20RPO%20Naczelny%20S%C4%85d%20Administracyjny%20-%20apostazja%2019.10.2017.pdf.

53 Judgment of 21 May 2018, I OPS 6/17, http://orzeczenia.nsa.gov.pl/doc/C7E540AFDB.

54 Supreme Court judgment of 15 January 2015, II CSK 747/13, not published.

55 B. Baran & K. Południak–Gierz, 'Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki', Zeszyty Naukowe Towarzystwa Doktorantów UJ Nauki Społeczne, 2017, No 2, p. 139–159.

in a case which ended with a judgment of the European Court of Human Rights (hereinafter "ECtHR").[56] In this judgment, the ECtHR stated that the court's refusal to order a newspaper to remove an article damaging the applicant's reputation from its internet archive constitutes no violation of article 8 ECHR. The theses were then repeated in the judgments of the Polish courts. For example, the Court of Appeal in Warsaw heard a case brought by J.G. against M.M. and Z.G. for the protection of personal rights.[57] The Court considered that since the internet publications fall within the press category and the task of the press is to describe events that are currently taking place, there are no grounds for the published articles to be monitored by the publisher or journalist as to their accuracy – even if the circumstances have changed. The press is not obliged to re-describe the issues raised earlier, and outdated articles can be a valuable source of information on the state of the art at a given time. Removing an article from the network would be a prohibited form of censorship and interference with the autonomy of the press by means of the possibility to collect and archive journalistic material. As a result, the Court of Appeal in Warsaw in this case accepted the line of argumentation presented in the ECtHR judgment. Polish courts also ruled similarly in other cases.[58]

Also the DPA used the concept of the right to be forgotten in its decisions, following the *Google Spain* judgment,[59] ordering the erasure of personal data. DPA in its decision of 2016, addressed to the Polish branch of US Facebook, enforced the erasure of personal data of the claimant processed illegally.[60]

Question 8

Article 85(1) GDPR sets out the competence of the Member States to adopt national provisions to reconcile the right to personal data protection and the right to information and freedom of expression. Paragraph 2 authorises Member States to provide for derogations or exceptions, indicating the scope of the provisions which may be affected.

56 Wegrzynowski and Smolczewski v. Poland (2013), ECLI:CE:ECHR:2013:0716JUD003384607.

57 Judgment of 17 June 2014 in a case I ACa 74/14; LEX No. 1515313.

58 Judgment of a Provincial Court in Warsaw of 10 July 2014, case VI ACa 19/13. For more: A. Grzelak, 'Prawo do bycia zapomnianym: dwa trybunały, różne stanowiska?', in L. Brodowski & D. Kuźniar-Kwiatek (Eds), *Prawo międzynarodowe a Unia Europejska. Księga jubileuszowa poświęcona Prof. E. Dyni*, Rzeszów, Oficyna Zimowit, 2015, pp. 102-112.

59 Judgment of 13 May 2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Google Spain)*, ECLI:EU:C:2014:317.

60 GIODO, 'Decision DOLiS 50/16 of 29 January 2016', di.com.pl/giodo-nakazuje-facebookowi-usuniecie-danych-pierwsza-taka-decyzja-wazna-dla-polakow-54404.

On the basis of article 85(2) GDPR, Poland introduced such derogations in PDPA.[61] According to article 2(1) PDPA, the provisions of articles 5-9, 11, 13-16, 18-22, 27, 28(2-10) and article 30 GDPR shall not apply to activities consisting in editing, preparing, creating or publishing press materials within the meaning of Press Law,[62] as well as the statements made as part of literary or artistic activities. The legislator interpreted GDPR term "journalistic purposes" as various kinds of press activities, defined by Press law. All press activities relate to press material, which is defined by article 7(2)(4) Press Law, as everything published, or conveyed to be published, in press text or picture of informational, publicist, documentary or other character, genre, form or purpose, regardless the medium.[63] The press clause excludes the application of certain rules of GDPR irrespective of the means of communication – journalistic activities concern not only the traditional press, but also radio, television or the internet.

This mainly concerns the following exemptions:

- exclusion of the rules on the processing of personal data, including (what may be particularly intrusive for the data subject in the context of his or her journalistic activities) the rules on the accuracy of data;
- exclusion of the application of provisions on the basis of data processing (except for information on convictions) – no consent is required for processing personal data for the purpose of editing, preparing, creating or publishing press materials; unless such a publication would concern the private sphere of life of the person whose data is the subject of publication, what stems directly from the prohibition introduced in article 14(6) Press Law;
- exclusion of the information obligation – as part of the press activity, it is not necessary to inform data subjects that their data are processed for the purpose of editing, preparing, creating or publishing press materials;
- limitation of the rights of the person whose data are processed in connection with the editing, preparation, creation or publication of press materials, including the right to access to their data, their rectification, limitation of their processing, transfer and data and the objection to the processing of their personal data.

However, neither GDPR nor PDPA excludes the right to be forgotten, other provisions regulating the status of data controller or general requirements regarding personal data security – privacy by default and privacy by design. However, from the point of view of

61 So called "press clause" were already included into PDPA97, however then it did not refer to academic expression. For more: M. Sakowska & A. Młynarska-Sobaczewska, '„Klauzula prasowa" z ustawy o ochronie danych osobowych jako gwarancja wolności wypowiedzi', Państwo i Prawo, 2005, No. 1, pp. 68-77.

62 JL 2018 item 1914.

63 M. Gawroński et al, 'Wyjątek dziennikarski (art. 2)', in: M. Gawroński (Ed.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa, Wolters Kluwer, 2018, p. 468.

the interests of a person whose data may be processed in connection with a press release – understood as a suspension of possible publication – it does not matter. In particular, the right to be forgotten – the right to erasure pursuant to article 17(3)(a) GDPR does not apply to the extent that processing is necessary, that means for the exercise of the right to freedom of expression and information.

The press clause should not be understood as an absolute exception to the application of GDPR – it applies only to journalistic activities, hence GDPR applies to all other processing of personal data not covered by the concept of journalistic activities. A journalist editing an article on negative marketing practices makes use of the press clause, but the same journalist, while carrying out marketing activities, cannot make use of such a privilege. This means that it is not the status of a person conducting business activity (a journalist), but the type of activity conducted – editing, preparing, creating or publishing press materials – that determines the exclusion from the application of certain provisions of GDPR and PDPA.

The Polish legislator slightly differently regulated the relation between GDPR and academic expression. According to article 2(2) PDPA, the provisions of article 13, 15(3) and (4), article 18, 27, 28 (2-10) and 30 GDPR shall not apply to academic expression.

C Domestic Enforcement of Data Protection Law

Question 9

Until 2018, the body responsible for personal data protection was GIODO, acting pursuant to PDPA97. The legislator decided, by the virtue of article 166 PDPA, to transform the institution of the GIODO into PUODO.[64] The person appointed for the post of GIODO remained in the office until the end of the term, from then on as PUODO. The new PUODO was nominated by Sejm in April 2019 and took on his duties on 16 May 2019.

The appointment process and structure of the DPA in Poland is regulated by PDPA.[65] According to article 34, PUODO is the authority competent in matters of personal data protection and acts as the supervisory authority within the meaning of GDPR, but also Directive 2016/680 and Regulation (EU) 2016/794 on the EU Agency for Law Enforcement Cooperation (Europol).[66]

64 Webpage of the Office, uodo.gov.pl/pl.

65 A. Grzelak & M. Wróblewski, 'Commentary to Chapter VI "President of the Office"', in M. Gumularz et al, (Eds), 2018, p. 261.

66 OJ 2016, L135/53.

PUODO is appointed and recalled by the Sejm upon the consent of the Senate for a 4 years term (renewal is possible only once). The term of office of PUODO expires only in situation directly foreseen in the legislation. PUODO performs his or her tasks through the Personal Data Protection Office (UODO), he may also appoint up to three deputies (currently only one deputy has been appointed). PUODO lays down the UODO's statute defining the internal organization and the scope of tasks of his or her deputies. PUODO nominates and dismisses his/her deputies. The staff of UODO (including directors of departments) is employed on the basis of 1982 Act on employees of state offices.[67]

According to article 48a PDPA, the Personal Data Protection Council, which is a consulting and advisory body, consisting of 8 members, shall be affiliated to PUODO. Up to now the Council has not been appointed by PUODO, although PDPA entered into force on 25 May 2018.

As for the enforcement record, there is no detailed and accurate information yet. Some of the decisions of PUODO are published on the webpage of the office.[68] Up till now (15 January 2020) eight financial sanctions were imposed (see question 11).

It should be also added that a separate supervisory structure has been established for courts and prosecutors' offices, acting as data controllers solely in the context of the administration of justice.[69] In that case, as a general rule, data processing is supervised by judicial authorities/senior prosecutors of a higher level. Finally, the National Council of Judiciary (NCJ) supervises the processing of data by the Tribunal of State, appellate courts, SC, SAC and the CC. As for the composition of the NCJ it should be noted that it is currently subject of controversy in the context of the rule of law principle.[70]

Moreover, the churches and religious associations which apply specific rules in accordance with article 91(1) GDPR shall be subject to supervision by an independent supervisory authority. For example, the Catholic Church established the Church Data Protection Supervisor (KIODO).[71] One should notice that the decisions of such organs are not subject to any judicial control in Poland at the moment.

67 The Act of 16 September 1982 (JL 2018 item 1915 as amended). Cf also article 113 PDPA.

68 PUODO, 'Decisions' uodo.gov.pl/pl/p/decyzje.

69 Art. 175dd of the Act of 27 July 2001 on the system of common courts (JL 2019 item 52 as amended) and art. 191 of the Act of 28 January 2016 on the prosecution service (JL 2019 item 740), as well as art. 1(3) PDPACrime.

70 Cf. judgment of 19 November 2019 in Joined Cases C-585/18, C-624/18 and C-625/18, *A. K. and Others v Sąd Najwyższy*, ECLI:EU:C:2019:982 or pending Case C-824/18, *Krajowa Rada Sądownictwa*. Cf. also Venice Commission, 'Opinion adopted at its 113th Plenary Session (Venice, 8-9 December 2017)', www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2017)031-e.

71 KIOD webpage, kiod.episkopat.pl/. List of other churches: www.uodo.gov.pl/pl/138/721.

Question 10

One cannot observe any of the DPA's strategies regarding the complaint handling task. There are no legal grounds to apply a strategy (in particular – prioritization) as regards complaints by PUODO. However, in January 2019 the yearly sector control plan was accepted by PUODO. Those cases are taken by PUODO *ex officio*. According to this plan, in 2019 PUODO shall verify the processing of personal data in areas such as: telemarketing, profiling in the banking and insurance sector or the waste identification and monitoring system. It will be also checked whether the disclosure of data in the Public Information Bulletin by entities obliged to do so does not violate the provisions on the protection of personal data. In the months to come, a closer look shall be taken at such entities as: police, border guard and detention centres, by checking their use of technical and organizational measures aimed at preventing unauthorized access, copying, changing or deleting data. Scheduled inspections are dictated mainly by numerous signals (including complaints, questions and reports of violations of personal data protection) indicating the threat of violation of the provisions on the protection of personal data in the above mentioned areas.[72]

Question 11

The system of personal data protection provides for a diverse system of liability: administrative, criminal and civil.

Starting with penal sanctions, the possibility to impose 'other penalties' (article 84 GDPR) was used by the legislator to enact penal sanctions in PDPA (articles 107 and 108). Still, as is it noted by commentators, one cannot exclude application of other sanctions of a penal nature (like disciplinary penalty) or sanctions interlinked with specific crimes, regulated by the Penal Code[73]. One shall however emphasize that the legislator was aware of the fact that the operation of the system of penal sanctions under PDPA97 was relatively inefficient. Therefore, PDPA introduced only three types of crimes regarding data protection. On the basis of PDPA, firstly, the data subject's right to informational self-determination is protected. Article 107(1) PDPA provides that any person who processes personal data, although processing thereof is not permitted, or is not authorized to process them, shall be subject to a fine, restriction of personal liberty or imprisonment for up two years. Article 107(2) lifts the imprisonment limit up to three years if the crime affects sensitive data. Secondly, the sound investigation activities of the personal data

72 PUODO, 'Plan', uodo.gov.pl/p/kontrole.

73 The Act of 6 June 1997 (JL 2018 item 1600 as amended). Cf. T. Banyś, in: M. Gumularz, K. Kozieł, P. Kozik, 2018, p. 469.

protection inspectors are secured by article 108(1). According to that provision, any person who prevents or hinders the inspector from checking the compliance with the personal data protection provisions shall be subject to a fine, restriction of personal liberty or imprisonment for up to two years. In May 2019, on the basis of GDPRImpl, a third type of crime was added. The same sanctions, as provided by article 108(1), shall apply to any person who does not provide the data necessary to determine the basis of the assessment of an administrative fine or who provides the data which make it impossible to determine the basis of the assessment of an administrative fine (article 108(2)).

Administrative fines, as regulated by article 83 GDPR and articles 101-105 PDPA, were applied by PUODO eight times by now (as of 15 January 2020). On 26 March 2019, by the virtue of an administrative decision,[74] an administrative fine of 943.700 PLN (around 225,000 EUR) was imposed on a company. The company in question processed data of persons obtained from publicly available sources (including the Central Register and Information on Business), and processed them for profit. The controller fulfilled the information obligation, providing information required by article 14(1-3) GDPR only to those persons with the established e-mail addresses. In case of other people, an information clause was posted on the website of the company. Therefore, the reason of the fine was a violation of the obligations enshrined in article 14 GDPR. The decision is at the moment subject of judicial control.[75]

Another financial penalty was imposed on 25 April 2019. The main reasons for the imposition of the penalty on the controller were ineffective attempts to remove the violation consisted of the publicizing of a too wide range of personal data.[76] The football association made public the personal data of the football judges who were granted the judges' licenses. Not only their names and surnames were public, but also their residence addresses and PESEL. By setting the fine – PLN 55 750.50 (around 12 800 EUR), account was taken of duration of the infringement and the fact that it concerned a large group of persons (more than 550).

The highest financial penalty (PLN 2 800 000, around 651 162 EUR) up till now was imposed on 10 September 2019.[77] The organizational and technical measures of personal data protection used by the company were not adequate to the existing risk associated with their processing, which resulted in leakage of data of approximately 2 million 200 thousand people. The company – according to PUODO – had no adequate procedures to respond in the event of unusual traffic in the network.

74 PUODO, 'Decision ZSPR.421.3.2018', uodo.gov.pl/360.
75 Cf. judgment of 11 December 2019 in Case II SA/Wa 1030/19, orzeczenia.nsa.gov.pl/doc/30EDD316DA.
76 PUODO, 'Decision ZSPR.440.43.2019' uodo.gov.pl/decyzje/ZSPR.440.43.2019.
77 PUODO, Information, uodo.gov.pl/pl/138/1189.

One of the penalties (PLN 40 000, around 9800 EUR) was imposed on the public organ. One of the reasons for imposing a penalty on the mayor of the city was that he did not conclude a contract entrusting the processing of personal data with the entities to which he provided these data. This applies, among others, to running the Public Information Bulletin and the software to create it. This decision of PUODO is also subject to judicial control at the moment.[78]

There is no information regarding triggering penal proceedings by the prosecution service on the basis of the information from PUODO or *ex officio*. However the proceeding initiated *ex officio* by PUODO on 21 August 2019, regarding the leakage of personal data of judges and their relatives by Ministry of Justice officials,[79] may lead to such proceeding.

Question 12

The concept of compensation for damages suffered for intangible harm has been developed in Poland by the virtue of Civil Code.[80] This Act protects personal goods, including legal measures sanctioning intangible harm (articles 23 and 24). According to article 24, any person whose personal interests are threatened by another person's actions may demand that the actions be ceased unless they are not unlawful. In case of infringement he/she may also demand that the person committing the infringement performs the actions necessary to remove its effects. On the terms provided for in Civil Code, he/she may also demand monetary compensation.

The above mentioned provisions of Civil Code may also be used, apart from other procedures, by the victims of personal data violations. Article 92 PDPA stipulates that in matters not regulated by GDPR, the provisions of Civil Code shall apply to claims related to the infringement of the personal data protection provisions referred to in articles 79 and 82 GDPR. That provision is interpreted as a referral to Civil Code regulations foremostly on delicts and the protection of personal goods.[81]

As regards the calculation of damages, the size of the harm done has fundamental significance – the suffering, pain or mental loss is decisive. The amount to be paid as a compensation should be significant for the victim and bring back emotional balance. The amount to be paid depends also on protected good, size of loss and its character. Therefore the purpose to remedy the damage is primary. The average economic conditions of the society have secondary significance.

78 PUODO, 'Decision of 18 October 2019', uodo.gov.pl/decyzje/ZSPU.421.3.2019.

79 PUODO, 'Decision ZSPU.440.1111.2019', uodo.gov.pl/pl/138/1148.

80 The Act of 23 April 1964 (JL 2019 item 1145).

81 P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa, Wolters Kluwer, 2018, p. 868.

Question 13

In Polish legislation, participation of NGOs in administrative process is foreseen by article 31 of the Code of Administrative Procedure (CAP).[82] An NGO can intervene in a matter involving another person with a request to commence proceedings, or to participate in proceedings, if such participation is justified by its statutes and where there would be a public benefit in allowing it. An NGO participates in proceedings with the rights of a party.

NGO's participation in judicial civil proceedings is regulated by article 61 CCP.[83] An NGO can in the field of their statutory tasks, with the consent of the individual expressed in writing, bring an action on its behalf in areas specified by CCP. In such cases NGO can in the field of their statutory tasks, with the consent of the individual expressed in writing, join the ongoing proceedings. Some of the commentators argued that CCP should be amended in order to make article 80 GDPR fully effective,[84] since it does not enumerate neither the data protection nor protection of privacy or personal goods as areas NGOs can play their role.

With regard to data protection law, the possibility given by article 80(2) GDPR has not been used to legislate on the right to lodge a complaint independently of a data subject's mandate. According to article 61 PDPA, an NGO – referred to in article 31 CAP – can also participate in the procedure upon the consent of the data subject, in its name and on its behalf. An NGO cannot act independently and its participation calls for subject's consent. As a consequence, NGOs in Poland in data protection cases cannot act exclusively in the public interest.

One shall point at the Foundation "Panoptykon" which, by today, is the most active NGO in the area of privacy and data protection. However, there are also other NGOs active partially in the field of data protection or access to information.

Question 14

For many years, GIODO cooperated closely with national Ombudsman (RPO). Apart from the shared perspective – protection of privacy and personal data as human rights – GIODO approached RPO in some cases regarding data protection, because of RPO's competences the data protection authority did not possess. Firstly, RPO is entitled to lodge complaints to CC – therefore GIODO having constitutional doubts regarding legislation

82 The Act of 14 June 1960 (JL 2018 item 2096 as amended).
83 The Act of 17 November 1964 (JL 2019 item 1460 as amended).
84 P. Litwiński et al, 2018, p. 816.

used to turn to RPO.[85] Secondly, RPO is entitled to lodge motion with the SC and SAC to decide in a 7 judges panel (or even the whole chamber) on divergences in case law, also regarding data protection.[86] GIODO did not possess such competences (the situation has not changed with PUODO).

It is uncertain whether this trend remains unchanged. One shall take notice of the exceptional (first after a decade) complaints of RPO, addressed to administrative courts, directed against PUODO's decisions forbidding publication of supporters' names for candidates to the new NCJ.[87] It is difficult to foresee how this delicate and partially constitutional issue, can influence the above mentioned trend.

There is no information or additional data as regards PUODO's cooperation with regulatory bodies, but it cannot be excluded.

D Data Processing for National Security Purposes

Question 15

There is no definition of "national security" in domestic legislation.[88] The obligation to ensure the national security shall secure fundamental values crucial for the very existence of the nation and the national identity. The pillar of the national security is the protection and defence of the nation's primary interests, such as national identity, territorial integrity and constitutional structure. This issue turned out to be controversial. According to article 6 PDPA, neither PDPA nor GDPR applies to: 1) processing of personal data by entities of public finance sector referred to in specific provisions of the Act on Public Finance, to the extent that processing is necessary to perform tasks aimed at guaranteeing national security, if special provisions stipulate necessary measures of protecting the rights and freedoms of the data subject; 2) activities of special forces within the meaning of article 11 of the Act on the Internal Security Agency and Foreign Intelligence Agency. Moreover, according to its article 3(2), PDPACrime is not applied to personal data processed in connection with the provision of national security, including the statutory tasks of the Internal Security

85 Cases K 33/13 (health registries) and K 25/13 (registry of marrow donors), brought before CC by RPO, were in fact initiated by GIODO's letter to RPO.

86 One example is the decision of SAC as of 21 May 2018, case I OPS 6/17, regarding processing personal data by Catholic Church, which was triggered by RPO. RPO, 'webpage', www.rpo.gov.pl/pl/content/nsa-odmowil-wydania-uchwaly-w-sprawie-kompetencji-giodo-wobec-apostatow.

87 RPO, 'Skarga', www.rpo.gov.pl/pl/content/rpo-skarzy-decyzje-puodo-ws-list-poparcia-kandydatow-do-krs.

88 J. Kurek, 'Zakres stosowania ogólnego rozporządzenia o ochronie danych osobowych i dyrektywy 2016/680/UE – wyzwania związane z wyodrębnieniem działań państwa w obszarze bezpieczeństwa narodowego i bezpieczeństwa publicznego', Europejski Przegląd Sądowy" 2017, No. 5, p. 43.

Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence and the Central Anti-Corruption Bureau. According to the doctrine, these exclusions are not only too broad in the absence of a definition of the term "national security", but also include institutions whose activities go far beyond the common understanding of the term. For example, the Central Bureau of Anticorruption is responsible for fighting corruption in public and economic life, in particular in state and local government institutions, but also for example in sport, as well as fighting activities detrimental to the economic interests of the state. This – in most cases – has nothing to do with national security.[89]

89 A. Grzelak (Ed.), *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*. Komentarz, Warszawa 2019, C.H.Beck, p. 52.

Portugal

Filipa Calvão and Clara Guerra[*]

A Setting the Scene

Question 1

In Portugal, the national legal instrument introduced to implement Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR") is Law 58/2019, of 8 August 2019. It also amends Law 43/2004 of 18 August 2004, that rules the composition, organisation and functioning of the National Supervisory Authority (hereinafter "NSA").[1]

It should be stressed that the late publication of the national implementing law prevented Portugal from having its data protection legal framework completed. This can explain some lack of doctrine and of case-law, resulting from somehow limited practical application of the GDPR.

It identifies the NSA, providing for similar provisions to those who have been ruling the constitution and activity of this public authority for the past two and a half decades with the novelty of recognising the NSA financial autonomy and legal personality (articles 3 to 5 of Law 58/2019). Moreover, the Portuguese NSA is the public authority entitled to supervise and monitor the compliance with the GDPR, the Law 58/2019 «as well as further legislative and administrative provisions related to data protection, in order to ensure rights and freedoms of individuals in the context of personal data processing».[2]

To accredit certification bodies the law appoints the national accreditation body designated in accordance with Regulation (EC) 765/2008 (article 14(1) of Law 58/2019).

There are some provisions on Data Protection Officers, in particular on the designation by public authorities or bodies (articles 9 to 13 of Law 58/2019), and also a provision related to article 8 GDPR, determining the age threshold of 13 years old (article 16 of Law 58/2019).

---

* Filipa Calvão: Associate Professor, Faculty of Law (Oporto School), Catholic University of Portugal; Researcher, Católica Research Centre for the Future of Law; President of the Portuguese Data Protection Authority. Clara Guerra: Senior Consultant, Portuguese Data Protection Authority; Guest Lecturer, Faculty of Law, Catholic University of Portugal.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Art. 4(2) of Law 58/2019 of 8 August 2019.

It also contains several provisions referring to the exercise of the right to remedies and liability (articles 32 to 35 of Law 58/2019).

It is important to highlight that, under recital 27 of the GDPR, the Portuguese law has extended to deceased persons the protection of personal data listed in article 9(1) of the GDPR and those related to private life, image and telecommunication (article 17 of Law 58/2019). On this aspect, the Portuguese legislator has partially reaffirmed the interpretation of the previous legal regimen on data protection based on the legal provisions of the Portuguese Civil Code that protect the personality of deceased persons (articles 71 and 80 of the Civil Code), just not covering personal data outside the special categories of data and outside data of a highly personal nature.

In what concerns the flexibilities provided for in the GDPR, apart from provisions related to the processing in the context of employment and health and genetic data (articles 28 to 30 of Law 58/2019), the Portuguese Law does not fully avail them.

In particular, the provision referring to the balance between data protection and freedom of expression and information does not provide for limits or specific guarantees, beyond those already reflected in the Portuguese Constitution (article 24 of Law 58/2019). In what concerns processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, it has derogated with no exception, and with poor guarantees, the rights referred to in articles 15, 16, 18 and 21 of the GDPR (article 31(2) of Law 58/2019). Also some rights provided for by the GDPR, such as the right to information provided by Article 13 and the right of access, are restricted by the national law in breach of the requirements stated by article 23 of the GDPR (article 20 of Law 58/2019).

Finally, there is a set of provisions on administrative fines that are in breach of the GDPR, concerning the infringements settled by article 83 (4) and (5), which were developed in articles 37 to 39 of Law 58/2019. On the one hand, the maximum amounts of administrative fines determined by article 83(4) and (5) of the GDPR are lowered, taking into account the nature of the controller or processor, in particular if it is an individual or a small and medium enterprise; on the other hand, the infringements that have a negligent character cannot be sanctioned by the NSA unless, after an "advise" to correct the situation, the infringements continue; in some cases negligent infringements are not sanctioned at all (e.g. infringement of the principles provided by article 5 of the GDPR).

In what concerns the Law 58/2019, the Portuguese SA has given a very critical opinion on its draft proposal during the legislative proceeding and has taken the resolution not to apply in its future decisions the provisions that are clearly in breach of the GDPR.[3]

3 Deliberação/2019/ 494 of 3 September 2019 of the Comissão Nacional de Proteção de Dados (hereinafter "CNPD"), www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2019&segunda_escolha=20. All webpages referred to were visited on 9 February 2020.

Question 2

The Portuguese Constitution differentiates, since its approval on 2 April 1976, the right to respect for private life and the right to data protection (articles 26 and 35, respectively), being the first written Constitution in the world to recognise the protection of personal data as a fundamental right.

Beyond the legal protection ensured by national civil law (article 80 of the Civil Code of 1966), the Portuguese Constitution recognises the respect for private life as a fundamental right in article 26(1) and (2) and provides for specific guarantees in the context of telecommunication in article 34(4).[4]

Article 35, with the title 'Use of computerized data', of the Portuguese Constitution of 1976 provided for a set of fundamental rights related to data processing through automated means, that intended to ensure the right to informational self-determination.[5],[6]

Later, by the revision of the Constitution that occurred in 1997 in order to adjust this article to Directive 95/46/EC, the material scope of this provision was extended to the processing of personal data other than by automated means.[7]

It is worthwhile mention that since its first wording, article 35 (3) relates both fundamental rights, specifying that private life is, among other personal data (sensitive data), subject to reinforced protection.[8]

Hence, the Charter of Fundamental Rights of the European Union (hereinafter "Charter") has not had such a significant impact in Portugal as it might have had in other Member-States.

Nevertheless, the Charter is frequently invoked for supporting the guarantee of the right to data protection before national courts as well as by the NSA, in particular in its written advices on drafts of legislative and administrative measures as well as in its concrete

4 Rectius, the Portuguese Constitution provides for the right to the *intimacy* of private and familiar life. Though this formulation seems to be more restricted than the one of the Charter of Fundamental Rights of the European Union, the truth is that the Constitutional Court has affirmed a broad interpretation of that right, covering also a patrimonial dimension of private life – see judgments 278/95 and 355/97, in www.tribunalconstitucional.pt/tc/acordaos/.

5 J.J. Gomes Canotilho &Vital Moreira, *Constituição da República Portuguesa Anotada*, 4th ed., Coimbra, Coimbra Editora, 2007, vol. I, pp. 551-556.

6 P. Ribeiro de Faria, 'Anotação ao artigo 35.º', *in* Jorge Miranda & Rui Medeiros, *Constituição Portuguesa Anotada*, 2nd Ed, Coimbra, Coimbra Editora, 2010, Vol. I, pp. 779-801.

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with the regard of the processing of personal data and on the free movement of such data [1995] OJ L281/31.

8 Explaining the history of this constitucional provision, see Joaquim Seabra Lopes, 'O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível', in *Forum de Proteção de Dados*, n.º 2, Jan. 2016, pp. 14-51, www.cnpd.pt/bin/revistaforum/forum2016_2/index.html. See also Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, pp. 695 ss.

decisions regarding the balance between that fundamental right and other rights or interests in conflict.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Before 2018, the national law that transposed Directive 95/46/EC (Law 67/98, of 26 October 1998) provided for the need to obtain a prior authorisation from the NSA to process sensitive data, as well as to further process data for new purposes. Therefore, only under GDPR application have data controllers started applying themselves directly these principles and processing data accordingly to their own assessment.

In this new context, most data controllers reveal difficulties in assuming this new task, especially in interpreting and applying the principles of purpose limitation and data minimisation.

With regard to purpose limitation principle, data controllers tend to a generous evaluation of the compatibility test between the original and the new purposes. In particular, when controllers are public bodies there has been an intense reaction from civil society signalizing an abuse in some cases of further processing for new purposes, which led to the correction of the processing or simply a more careful and rationalized decision for future processing of data.

As to the data minimisation principle, data controllers tend to have increased difficulties in implementing it. The same occurs with the implementation of the storage limitation principle. Actually, praxis reveals a tendency to collect and store more data than necessary for the specified purpose of the processing as well as a difficulty to determine the adequate period of retention and to justify the option made.

For a better application of those principles, the Portuguese SA issued guidelines on specific kinds of data processing – most of them still under the Law that transposed Directive 95/46/EC – developing and adjusting the interpretation made by Article 29 Working Party and by the European Data Protection Board (EDPB), to the specificities of the national legal order, in particular in some sectors of activity.

Furthermore, the NSA has issued decisions advising moderation on the reuse of data for other purposes than the one for which personal data had been collected.

Although so far there are no judgements by the Portuguese Courts under the GDPR, as the principles remain unchanged in relation to Directive 95/46/EC, the following should be noticed: domestic Courts do not ignore the guidelines of Article 29 Working Group nor of the Portuguese SA, given that the parties involved in the process do usually invoke

them in their submissions, and in most cases share the same perspective; in spite of that, the case-law is not always in accordance with the interpretation of the NSA.[9]

Question 4

As already pointed out, there are no judgements by the Portuguese Courts under the GDPR until now, so the national Courts' interpretation on the legal basis for data processing is related to the legal basis provided for by the law that transposed Directive 95/46/EC (Law 67/98), which is similar to the conditions of lawfulness provided for by the GDPR.

In this context, the case-law shows some discrepancies on the evaluation of the attributes of consent, particularly with regard to the legal requirement of specific consent (e.g., consent given by a person for access to his/her health data by insurance companies).[10]

With respect to legitimate interests there are not many judicial decisions, in part because the balance between data protection and other interests, like administrative transparency or the exercise of a right in a judicial process, is done by the Courts on the grounds of other specific laws. Furthermore, regarding legitimate interests in the digital environment, although there are some interesting judgments on the disclosure and on the reuse of personal data in the context of social networks, the majority of the case-law focuses on the right to respect of private life and not on the right to data protection and its specific legal regimen[11].

On balancing of interests, it should be highlighted a judgement by the Court of appeal, forbidding parents to disclose photographs or any other information that could lead to the identification of their child in social media, on the grounds of the prevalence of private life and data protection over the freedom of expression of the parents, in the name of the superior interest of the child.[12]

9 About the proportionality of the data retention period, see the judgment of the Supreme Administrative Court of 21 March.2019, Proc. No. 220/17, at www.dgsi.pt.

10 See the judgment of the Supreme Administrative Court of 08 August 2018, Proc. No. 0394/18, at www.dgsi.pt,. Concerning the access by a third party to health data, the Court ruled that it should only be given access to the data expressly covered by the statement of consent. About consent, see also Alexandre Sousa Pinheiro, 'Anotação ao artigo 4.º, 11)', *in* Alexandre Sousa Pinheiro (Ed.) *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, pp. 166-173.

11 Within this context, following the criteria of the expectation of privacy, see, for all, the judgment of *Tribunal da Relação do Porto* (an intermediate court of appeal) of 08 September 2014, Proc. No. 101/13.5TTMTS.P1, at www.dgsi.pt.

12 Judgment of *Tribunal da Relação de Évora* (an intermediate court of appeal) of 25 October 2015, Proc. No. 789/13.7TMSTB-B.E1, in www.cnpd.pt/bin/revistaforum/forum2016_2/index.html.

Question 5

In regard to the validity of personal data as 'counter-performance' for the provision of digital content, this issue has been debated in Portugal, mainly in the context of conferences and seminars.[13]

Recently the new Law 58/2019 has contributed to this debate through a provision that seems to admit that the legitimacy of processing personal data *necessary* for the performance of a contract might be found on consent. Actually, article 61(2), regarding data processing that existed prior to the application of the GDPR, intends to ensure that consent fulfils the attributes provided for by article 4(11) of the GDPR, determining the end of a contract to which the data subject is party if the consent is not in accordance with the GDPR. Although this provision is not necessarily headed to contracts on digital services or goods, yet it has surely the consequence of generating confusion on an issue that seemed relatively pacified by the GDPR.

It should also be highlighted that the NSA has decided not to apply in concrete cases that national provision on the ground that is in breach of articles 4(11) and 6(1)(a) and (b) of GDPR.

Question 6

In what concerns the rights provided by the GDPR to data subjects, the Portuguese Law is quite restrained. Actually, Portugal did not introduce so far any national legislative measure concerning automated decision-making, making use of the possibility provided by article 22(2)(b) of the GDPR.

Question 7

With regard to the right to erasure towards search engines, the NSA has handled some requests from data subjects in order to have their right guaranteed, following standard answers received from the data controllers denying to de-list the results presented when searching by a name, always invoking public interest in providing such information, regardless of the context or the notoriety of the person concerned.

13 About the difficulties to legitimate the colletion of personal data in the digital environment under the GDPR, see also A. Leal Alves, 'Aspetos jurídicos da análise de Dados na Internet (Big Data Analytics) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação' in A. Menezes Cordeiro et al. (Eds), *FinTech. Desafios da Tecnologia Financeira*, Coimbra, Almedina, 2017, pp. 75-150.

In general, the NSA did not recognize the arguments of the companies, for going much beyond the interpretation of the CJEU ruling in the Case *Google Spain*; therefore, it decided in favour of the data subjects and it issued deliberations ordering the de-listing.[14,15]

The search engines either complied with the NSA decision or challenged it in the court, there being no apparent reason for the different ways taken. Those cases are still pending at the national courts.

Still in respect to the right to erasure, national law implementing the GDPR has notably introduced a provision on how this right can be ensured when personal data is published in the official journal.

It states that the right to erasure of personal data published in the official journal has an *exceptional nature* and can only be applied in the conditions laid down by article 17 of the GDPR in the cases where it is the only way to safeguard the right to be forgotten, after due balance of the interests at stake. This is done through the deindexation of personal data from the search engines, but always without erasure from the official publication (article 25(4) and (5) of Law 58/2019).

It is also determined by this law that, in case of publication of personal data by the official journal, the data controller is the body requesting the publication (article 25(6) of Law 58/2019).

Definitely, there is no right to erasure from the official journal, but a right, in certain circumstances, not to have the personal data published by the official journal processed by search engines. This is exercised not directly towards the search engines, as data controllers, but has to be exercised via the official journal which is the body that controls the online publication and is able to make the deindexation, yet not being the data controller.

Question 8

About national legislative measures to reconcile the right to data protection with the right to freedom of expression, Portugal did not really regulate how this balance could be achieved nor did introduce any actual derogations. Article 24 of Law 58/2019 disposes that the GDPR and national rules on data protection are without prejudice of the freedom of expression and of the freedom of information and of the press. It provides in general terms that the exercise of the right to information shall respect the principle of human dignity

14 Judgment of 13 May 2014, in Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Google Spain), ECLI:EU:C:2014:317.

15 About the grounds for the decisions of the Portuguese SA, see J. Marques, 'Direito ao esquecimento. A aplicação do acórdão Google pela CNPD', in *Forum de Proteção de Dados*, No. 3, July, 2016, pp. 48-55, in www.cnpd.pt/bin/revistaforum/forum2016_3/index.html.

and the personality rights, in particular whenever discloses special categories of data or personal data of deceased persons.

Then a specific provision affords special protection to data subjects' addresses and contacts, expressly providing that the right to freedom of information does not legitimate such disclosure, unless when data is already of public knowledge (article 24(4) of Law 58/2019).

The GDPR implementing law introduced though a clear distinction between data processing within freedom of expression and data processing for journalistic purposes, when requiring that in the latter case such processing shall comply with national law on access and exercise of the professional journalism.

In Portugal there is already specific legislation regulating the activity of the press and other social communication means, including journalists' activity, and there is a dedicated independent regulator to monitor compliance with such legal framework. However, such legislation does not contain any provisions on personal data protection or provide for the exercise of GDPR data subjects' rights.

It should be noted, in this context, that the Press Law[16] provides that the freedom of the press is only limited by the Constitution and the law, in order, namely, to ensure the accuracy and objectivity of the information and to guarantee the rights to good reputation, intimacy of private life and image.

Apart from these general restrictions, which can be related to the processing of personal data, there are no other provisions intended to strike the balance between data protection and the freedom of expression and information.

C Domestic Enforcement of Data Protection Law

Question 9

In what regards the national enforcement of data protection law, it should be underlined that the Portuguese data protection supervisory authority is Comissão Nacional de Proteção de Dados (hereinafter «CNPD»).[17]

It is an independent administrative legal body with powers of authority and administrative and financial autonomy that operates within the Parliament. Its composition, statute and staff are approved by law of the Parliament.

The CNPD is a public legal person directed by a collegiate body, composed of seven members of recognized merit and integrity: one President elected by the Parliament; two

16 Art. 3 of Law 2/99, of 13 January 1999.

17 Arts. 3 to 6 of Law 58/2019 and Law 43/2004, amended by Law 58/2019.

members elected by the Parliament by Hondt's highest average rule; one judge appointed by the Judiciary Superior Council and one magistrate from the Public Prosecutor's Office appointed by its own Superior Council; two members appointed by the Government.

The members have a five-year mandate that can be renewed twice. They take office before the President of the Parliament. All activities, paid or unpaid, are considered incompatible with the NSA membership, with the exception of teaching in the University and researching. The CNPD acts with independence when fulfilling its tasks and exercising its powers.

The CNPD is provided with its own staff, only bound by the general rules governing public administration.

The national law implementing the GDPR provides for the following additional competences for the NSA: to issue non-binding opinions on draft legal instruments in preparation at European or international institutions related to personal data protection; to monitor the compliance of the GDPR and other legal provisions on the protection of personal data and of the rights, freedoms and guarantees of the data subjects, as well as to correct and sanction any non-compliance; to define criteria allowing to densify the concept of 'high risk' referred to in article 35(4), in connection with the list of data processing operations requiring a Data Protection Impact Assessment; to draft and submit to the EDPB the criteria for the accreditation of the monitoring bodies for codes of conduct and of the certification bodies, pursuant articles 41 and 43 of the GDPR; to cooperate with the National Accreditation Body (IPAC, IP), entrusted with the task provided by article 43(1)(b) of the GDPR, in particular in the definition of additional requirements for accreditation.

In what concerns enforcement under the GDPR, for the period 25 May 2018-31 July 2019, the NSA presents the following statistics:[18]

- Number of investigation proceedings (resulting from complaints, referrals from other national authorities and the NSA's own initiative): 1075
- Number of data breaches notifications (article 33 GDPR): 326
- Number of inspections on the spot: 325
- Number of organisations (public and private) to which fines were applied: 5
- Total amount of the fines applied: ± 425 000 euro

Besides the enforcement activity carried out at national level, the consistency mechanism provided by the GDPR has brought a new line of work requiring involvement of NSAs upon the likelihood of data subjects in that Member State being affected by data processing even when there is no establishment of the controller in that territory. Consequently,

18 These figures were provided by CNPD for the 1st anniversary of GDPR application and then updated with reference to the end of July, in a time frame of 14 months still with no national GDPR implementing law.

additional efforts on enforcement are required. In spite of being not converted into these statistics, they have a real impact on the enforcement activity at national level.

Question 10

As to the strategy of the NSA for complaints-handling, it is important to recall that the right to data protection is a fundamental right, not only recognised by the Charter but also by the Portuguese Constitution.

Therefore, there is a legal obligation to ensure to each individual that his/her rights are guaranteed. In view of the possible great amount of complaints, several strategies can be envisaged to handle complaints in an effective manner, such as sorting them according to similarity, planning inspection activities having due account of the main or recurrent problems detected or redefining internal working methods to cope with new scenarios.

However, the Portuguese SA cannot, according to the national legal order, ignore complaints based on an assessment of minor pertinence of the complaint. In fact, all admissible complaints have to be dealt with, according to the law, since it imposes such obligation to the NSA leaving no margin of discretion.

Though prioritization is indispensable, mainly because of the lack of resources of the NSA to fully comply with its tasks, it cannot lead to setting aside a case where a fundamental right of an individual is or might be at risk. In that sense, the effectiveness in the action of the NSA cannot be affirmed with prejudice to fundamental rights.

Question 11

Law 58/2019 adds sanctions to those explicitly provided for by the GDPR, maintaining a tradition of recognising criminal relevance to some infringements of data protection provisions: further processing of personal data for a purpose incompatible with the initial purpose; undue access to personal data; invalidation or destruction of personal data; data deviation; entry of false data; violation of the duty of secrecy; non-compliance with an order of the NSA (articles 46 to 52 of Law 58/2019).

Besides criminalising those conducts, national law also provides for administrative fines for some infringements of the GDPR not covered by article 83(4) and (5) of the GDPR: the infringement of articles 10 and 41(4); and the monitoring of codes of conduct by bodies not accredited by the NSA – articles 37(1)(e) and 38(1)(q) and (r) of Law 58/2019.

The Law, in article 37(1)(l), also sanctions with administrative fines the infringements of the limits and conditions stated on its chapter VI, relating to specific processing operations under articles 85 to 89 of the GDPR.

As mentioned supra, Law 58/2019 has provisions that are in breach of the GDPR, concerning the infringements settled by article 83(4) and (5). The Portuguese legislator determined different maximum amounts of administrative fines from the ones provided in the GDPR, depending on the controller or processor being an individual or a small and medium enterprise – articles 37 (2) and 38(2). Besides, the national implementing law prevents the NSA to sanction negligent infringements unless, after an "advise" to correct the situation, the infringements continue – article 39(3). Though having replicated the list of infringements provided by article 83(4) and (5), it has omitted the negligent infringement of the principles provided by article 5 of the GDPR, reducing the provision to an intentional infringement.

In what regards the exercise of corrective powers by the Portuguese SA, it should be noticed that such powers are not, in fact, new in the national legal order. The previous data protection law (Law 67/98) already endowed the SA with corrective powers, specifying the power to apply administrative fines. The only difference has to do with the legal framework of the administrative fines, which is now much more impressive than the one provided by the Portuguese law twenty years ago.

Despite the fact that the national law that implements the GDPR is in force only since 9August 2019, the CNPD has been exercising the powers provided by the GDPR on the ground that the Law 67/98 had not been implicitly revoked in full, keeping in force the national provisions that did not contradict the GDPR, in particular the one that appointed the CNPD as national SA.

Therefore, during the past year the CNPD has applied, under the GDPR, several corrective measures mainly to data controllers, among which stands out four decisions sanctioning data controllers.[19]

Question 12

Article 82 of the GDPR, providing data subjects for a right to receive compensation for material or non-material damages as a result of an infringement of the GDPR, does not represent a real innovation in the Portuguese legal order.

Indeed, the previous data protection law (Law 67/98) already provided for the right to compensation, and it was interpreted combined with further legal provisions that specified the coverage of non-material damages.

Article 496 of the Civil Code (of 1966) and article 3 of the Rules of non-contractual civil liability of State and other Public Entities, approved by Law 67/2007, of 31December

19 See Deliberação 984/2018, in www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf and Deliberação/2019/21, Deliberação/2019/207 and Deliberação/2019/222, www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2019&segunda_escolha=20.

2007, provide for the compensation for non-material damage, although limiting it to the damages that, for its gravity or seriousness, deserve legal protection. This last precision, explicitly stated in article 496 of the Civil Code, has been interpreted as to exclude the minor harm – and this is the only aspect of national law that may raise some difficulties in ensuring the implementation of article 82 of the GDPR in accordance with the case law of the CJEU, according to which "Reparation for loss or damage caused to individuals as a result of breaches of Community law must be commensurate with the loss or damage sustained so as to ensure the effective protection for their rights".[20] However, there are some Portuguese authors that consider this national legal requirement as a short add, since it has to be evaluated in each concrete case.[21]

Hence, Portuguese Courts have long condemned those who inflicted non-material damages, taking into consideration not only physical pain and emotional suffering, but also damage caused by the disclosure of facts related to private life.[22]

More recently there are judgments recognising the right to receive a compensation for the infringement of provisions that protect personal data.[23]

In what concerns the criteria for calculating such damages, the case-law follows an "equity judgment", taking into account the degree of fault as well as the economic situation of both the one who inflicted the damage and the injured person.[24]

Question 13

Concerning the information and power asymmetries between data controllers and data subjects and the purpose of the EU legislator to mitigate them by providing for the possibility of representative actions pursuant to article 80 of the GDPR, it is important to

20 Judgement of 5 March 1996 in Joined Cases C-46/93 and C-48/93, *Brasserie du Pêcheur SA v. Federal Republic of Germany and The Queen v. Secretary of State for Transport, ex parte Factortame Ltd and Others,* ECLI:EU:C:1996:79, para 82.

21 See M. Rebelo de Sousa & A. Salgado de Matos, *Direito Administrativo*, 2nd ed., Lisboa, D. Quixote, Ed., 2009, Vol. III, p. 496.

22 See, for instance, the judgment of the Supreme Court of Justice of 3 November 2016, Proc. No.323/12.6TVLSB,L2.S1, recognizing the right to compensation for non-material damages caused as a result of negligent breach of the duty to store a video that registered an intimate moment between the legitimate holder of the video and the person injured.

23 See the judgement of the Supreme Court of Justice of 16 October2014, Proc. No.679/05.7TAEVR.E2.S1, in a case where privacy and reputation of several data subjects (civil servants) was at stake as a result of the disclosure of personal data by the intentional action of a public office holder (notice that such data disclosures were judged, in the prior criminal law suit, as infringements to criminal law provisions related to data protection).

24 See the judgement of the Supreme Court of Justice of 4 May2010, Proc. No. 256/03.7TBPNH.C1.S1, at www.dgsi.pt.

recall that the new legal framework is very recent, being still difficult to assess potential trends in civil society in this regard.

Portugal does not have in general a high level of involvement of NGOs in representative actions. However national administrative law and administrative process law recognise to associations their legitimacy to defend 'collectively' the individual interests of its members provided that those interests are covered by the object matter or scope of the association. This possibility has been availed by unions to complain or report to the NSA infringements of data protection legal regimen, but seems insufficient – without a mandate from the data subject – to the exercise of the right to redress.

National law implementing the GDPR does not further develop Article 80 (1) of the GDPR, only admitting representation through a mandate of the data subject (Article 35 of Law 58/2019). Nevertheless, it is predictable that such kind of actions may significantly increase in the near future.

Question 14

In what concerns the intervention of further regulatory agencies or public authorities in data processing related complaints, it should be highlighted that in Portugal the supervision of data protection issues has been centralised in the CNPD for the last 25 years. Even in the e-Privacy legislation, where there are shared competences with the telecom regulator, the competences are well distinguished and data protection matters are only assigned to the NSA.[25]

In view of that, other regulators or authorities usually forward to the NSA complaints related to data protection and, moreover, they report to the NSA facts found in their own investigations, such as in the employment context, economic activities, consumer protection, financial sector and so forth.

The NSA has also a cooperation mechanism with the Ombudsperson in place for several years, for the exchange of information and complaints handling. Furthermore, there are some bilateral discussions with public bodies dealing with convergent matters to data protection and privacy, such as ethics, scientific research, e-voting and the national statistic system. Especially after the GDPR, informal cooperation between the NSA and Regulatory Agencies has increased, due to the consciousness of the importance to avoid contradictions in its respective guidelines or administrative measures.

25 Law 41/2004, of 18 August 2004, as amended by Law 46/2012, of 29 August 2012.

D Data Processing for National Security Purposes

Question 15

There is no legal definition of 'national security', but it is commonly perceived that national security is ensured by intelligence services, due to their tasks, and not by law enforcement authorities. Consequently, as there is a constitutional prohibition for the intelligence services to carry out any criminal prevention or investigation, the scope of the application of Directive 2016/680 and its transposition into national Law 59/2019, of 8 August 2019, make it clear that excluding national security means in Portugal excluding the intelligence services from the application of the Law Enforcement Directive (LED).[26,27]

The intelligence services (SIRP) are regulated by specific legislation and their activities are supervised by two different bodies: a parliamentary oversight commission and another body composed of magistrates to monitor some aspects of the data processing, including the exercise of the rights of the data subjects.

Being the right to data protection a fundamental right in Portugal since 1976, the first data protection law, dated from 1991 (Law 10/91 of 10 January 1991), already covered the law enforcement sector with the same data protection rules as the other public bodies and private organizations, with only two derogations concerning the right to information and the right of access which had specific provisions.

Actually, apart from the intelligence services, all other sectors were governed by the same data protection legal framework. Therefore, though the terminology might be confused, especially when used in European legal texts for different national contexts, the waters have been divided so far. It should be noted though that while excluding national security from its scope of application, the LED invokes 'national security' as one of the possible grounds to restrict data subjects' rights. The national law transposing the LED follows the same misleading legal provision, what might bring problems of interpretation and application of the law.

In what regards the national data retention law – Law 32/2008, of 17 July 2008 – its purpose is restricted to the prevention, detection and investigation of serious criminal infractions, by competent authorities, exactly like the subject matter and scope of the

26 'National security' is stated in art. 15 of the e-Privacy Directive (Directive 2002/58/EC) as meaning «State security». Without giving a definition, the European legislator clearly intended to determine the scope of national security.

27 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

Directive itself, which on the other hand refers to the national legislation. According to the Portuguese data retention law, only a limited number of listed law enforcement authorities can have access to the data retained to strike serious crime after a judicial warrant. Within this law, there is no use of data for national security purposes or access to data by intelligence services.[28]

Nonetheless, the national data retention law, after the CJEU ruling that invalidated the Data Retention Directive, is to be considered in breach of the Charter, regardless of the purpose for which the data is retained and further accessed.[29]

The NSA has expressed this view immediately after the invalidation of Directive 2006/24/EC and, after Tele 2 Judgement, it has deliberated not to apply the national data retention law for being in violation of EU Law.[30,31,32]

With the Portuguese Data Retention Law still in force, the Parliament passed a specific law to grant access by the intelligence services to the data retention database. The NSA gave a negative opinion during the legislative proceeding and the law was considered unconstitutional by the Constitutional Court in 2015, following a constitutionality prior check.[33,34]

A second law was passed, on which the CNPD issued a negative opinion as well. The Constitutional Court found it partially unconstitutional.[35,36]

In the meantime, the Ombudsperson requested the Constitutional Court to evaluate whether the national data retention law was in accordance to the Portuguese Constitution, including in what concerns the respect for the primacy of the EU law. Such request is still pending for assessment.[37]

---

28 Law 32/2008 is the Portuguese law transposing Directive 2006/24/EC. In spite of the Directive had been invalidated by the CJEU, the national law is still in force in Portugal.

29 Judgement of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* (Digital Rights Ireland), ECLI:EU:C:2014:238.

30 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

31 Judgement of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Tele 2), ECLI:EU:C:2016:970.

32 Deliberação 641/2017 of the CNPD, www.cnpd.pt/bin/decisoes/Delib/20_641_2017.pdf and Deliberação 1008/2017 of the CNPD, www.cnpd.pt/bin/decisoes/Delib/20_1008_2017.pdf.

33 Parecer 51/2015 of the CNPD, www.cnpd.pt/bin/decisoes/Par/40_51_2015.pdf.

34 Judgement 403/2015 of the Constitutional Court, www.ribunalconstitucional.pt/tc/acordaos/20150403.html.

35 Parecer 38/2017 of the CNPD www.cnpd.pt/bin/decisoes/Par/40_38_2017.pdf.

36 Judgement 464/2019 of the Constitutional Court, www.tribunalconstitucional.pt/tc/acordaos/20190464.html.

37 Request from the Ombudsperson of 26 August 2019, www.provedor-jus.pt/?idc=32&idi=18045.

In spite of the national legal framework being clear in respect to the law enforcement and the national security activities, not affecting the scope of application of the LED, it is evident that there is an increasing trend to use data, primarily processed for commercial purposes, for law enforcement purposes in a massive and disproportionate way, and then becoming also available for access and further processing by national security agencies.

Romania

Augustin Fuerea and Roxana-Mariana Popescu[*]

A Setting the Scene

Question 1

As regards the measures for the application of the General Data Protection Regulation (hereinafter "GDPR"),[1] the following national legislation is of relevance:

1 Law no. 129/2018 amending and supplementing Law no. 102/2005 regarding the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing, as well as repealing Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data.[2] Following legislative interventions, Law no. 102/2005 was republished in the Official Gazette no. 947 of 9 November 2018.

The new legal framework:

- strengthens the independence and autonomy of the Supervisory Authority in line with the GDPR requirements;
- provides for the exercise of the monitoring and control competences and duties of the Supervisory Authority and the compliance of the specific rights of natural persons in accordance with the provisions of the GDPR;
- establishes a new chapter dedicated to "Exercising the duties of control and complaint-handling" which sets out the main aspects regarding the carrying out of investigations and the settlement of the complaints addressed to the Authority;
- regulates an express procedure for conducting an investigation by the Supervisory Authority in the event that the controlled entities prevent such action;

---

* Respectively Professor and Associate Professor, Faculty of Law, Nicolae Titulescu University, Bucharest, Romania. The authors would like to thank the assistance received from the National Authority for Supervising the Processing of Personal Data, the National Authority for Consumer Protection, the Ministry of Communications and Information Society, as well as the Ministry of Internal Affairs (Directorate for Persons Record and Databases Management).

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

2 Official Gazette no. 503 of 19 July 2018.

- establishes the main contravention sanctions that can be applied, namely the warning and the fine, as well as the corrective measure with a novelty, under the form of admonition;
- provides legal remedies against the measures ordered by the Supervisory Authority, both for the operators and for the persons concerned;
- provides for transitional provisions in the context of repealing Law no. 677/2001, as follows:
  - The GDPR applies to complaints and notifications filed and registered with the Supervisory Authority from the date of its application, as well as to those filed before May 25, 2018 and which are now being solved.
  - Investigations initiated before May 25, 2018 and not yet completed, are subject to the GDPR provisions.
  - The finding of facts and the application of corrective measures, including contravention sanctions, after May 25, 2018, shall be carried out in accordance with the GDPR provisions and the legal provisions for its implementation.

2 Law no. 190/2018 on the implementation of the GDPR[3]

Most importantly, this law:

- expressly mentions the public authorities and bodies to which the GDPR provisions are applicable;
- the Chamber of Deputies and the Senate, the Presidential Administration, the Government, the ministers, the other specialised bodies of the central public administration, the autonomous public authorities and institutions, the authorities of the local public administration and those at county level, other public authorities, as well as the subordinated and/or coordinated institutions; are assimilated to the public authorities and/or bodies and worship units and associations and foundations of public utility;
- defines a number of terms such as: national identification number, remedial plan, remedial measure, remediation deadline;
- establishes special rules for the processing of certain categories of personal data, such as genetic data, biometric data or health data;
- establishes conditions for the processing of a national identification number (e.g. Personal Identification Number);
- establishes specific provisions on the processing of personal data in the context of labour relations;

3 Official Gazette no. 651 of 26 July 2018.

- provides for derogations for processing done for journalistic purposes, academic, artistic or literary expression, or for purposes of scientific, historical, statistical research, archiving in the public interest;
- mentions the terms of appointment and tasks of the Data Protection Officer, especially in case of public authorities and/or institutions and public bodies;
- designates the Romanian Accreditation Association (hereinafter "RENAR") as the national accreditation body for the certification bodies referred to in article 43 of the GDPR;
- establishes the derogatory sanctioning regime, including pecuniary sanctions, applicable to public authorities and bodies, giving priority to the prevention mechanism prior to the application of the fines.

It is important to mention, regarding the provisions of article 83(7) of the Regulation, that, as far as the public authorities or institutions are concerned, the Law establishes a mechanism of sanctioning them in a first stage, by applying the sanction with warning and by establishing a remediation plan. This step can be followed by the application of administrative sanctions, expressly provided by Law no. 190/2018 insofar as the public authorities or institutions have not fully implemented the measures provided in the remediation plan.

At the same time, regarding the certification bodies, it is necessary to specify that the normative act establishes that the accreditation of certification bodies, provided in article 43 of the Regulation, is performed by the Romanian Accreditation Association - RENAR, as a national accreditation body, in accordance with Regulation (EC) no. 765/2008,[4] as well as in accordance with Government Ordinance no. 23/2009 regarding the activity of accreditation of conformity assessment bodies, approved with amendments by Law no. 256/2011.

3 Decision no. 133/2018 regarding the approval of the procedure for receiving and solving complaints[5]

The significant changes in the conditions of admissibility and resolution of complaints by the Supervisory Authority, including in the context of cross-border processing, as a result of the entry into force of the GDPR and Law no. 102/2005, republished, led to the issuance of Decision no. 133/2018. Most importantly, this Decision provides that:

4 Regulation (EC) no. 765/2008 of the European Parliament and of the Council of July 9, 2008 establishing the accreditation and market surveillance requirements regarding the marketing of products, and repealing Regulation (EEC) no. 339/93 [2008] OJ L218/30.

5 Official Gazette no. 600 of 13 July 2018.

- complaints may be filed by any person concerned, especially if his or her habitual residence or place of work is in Romania or where the alleged violation has occurred on Romanian territory;
- complaints may be filed at the headquarters of the Supervisory Authority or transmitted by post, including electronic mail, or by using the electronic complaint form available on the institution's website[6];
- complaints may be filed personally or through a representative, including through a non-patrimonial organisation active in the field of personal data protection;
- petitioners are informed in writing about the admissibility of their complaint, including whether a more detailed investigation or coordination with other supervisory authorities will be carried and about the progress and outcome of the investigation;
- where the person concerned is dissatisfied with the way the complaint has been handled, she can address to the administrative court of the competent tribunal, after having gone through the preliminary procedure provided by the Administrative Contentious Law no. 554/2004[7], with subsequent amendments.

4 Decision no. 161/2018 regarding the approval of the procedure for carrying out the investigations[8]

This Decision establishes the conditions for carrying out investigations in the field, at the headquarters of the Supervisory Authority or in in writing, as well as their performance at the public authorities and/or bodies.

The investigation can be finalised by drawing up a report of finding, the imposition of a sanction or a decision of the President of the Supervisory Authority, providing for corrective measures and/or penalties can be ordered (warning, fine). In the case of public authorities and/or bodies, a warning is issued before a pecuniary sanction and a remedial plan is drawn up in accordance with the model provided by Law no. 190/2018, which must be complied with within the deadline set by the Supervisory Authority.

The measures can be challenged within 15 days at the administrative court of the competent tribunal.

5 Decision no. 128/2018 on the approval of the standard form for the notification of the personal data violation in accordance with the GDPR[9]

This Decision establishes the standard notification form for the personal data violation, in application of article 33(1) GDPR obliging the operators to report a violation of the

6 www.dataprotection.ro.
7 Official Gazette no. 1154 of 7 December 2004.
8 Official Gazette no. 892 of 23 October 2018.
9 Official Gazette no. 557 of 3 July 2018.

Supervisory Authority without undue delay and, if possible, within 72 hours from the date on which it became aware of it. The standard form is available on the institution's website **and can be transmitted electronically**.[10]

6 Decision no.174/2018 regarding the list of operations for which the assessment of the impact on the protection of personal data is mandatory[11]

This Decision was issued to ensure effective protection of the rights of individuals whose personal data are processed, especially in the case of certain personal data processing operations that pose risks to the rights and freedoms of individuals due to the nature of the data processed (e.g. sensitive data such as genetic, biometric, health data), scope, context and purposes of the processing, the specific nature of the categories of targeted people (e.g. vulnerable people, such as employees, minors), their number and/or the mechanisms used for data processing, especially those based on the use of new technologies.

The processing of data in the situations covered by this Decision obliges the operators to carry out a data protection impact assessment in accordance with article 25 of the GDPR.

7 Decision no. 99/2018 regarding the cessation of the applicability of normative acts of administrative nature issued in application of Law no. 677/2001 on the protection of natural persons with regard to the processing of personal data and the free movement of such data[12]

In view of the necessity of a predictable and clear legal framework, in accordance with the normative legal regulations, Decision no. 99/2018 was issued. It was also issued in the light of the European Commission's Communication to the European Parliament and the Council of 24 January 2018 entitled "Enhanced Protection, New Opportunities - Commission Guidelines on the Direct Application of the General Data Protection Regulation of 25 May 2018", specifying that "(w)hen adapting their national legislation, the Member States must take into consideration any national measures that would result in an obstacle to direct application of the regulation and jeopardising its simultaneous and uniform application across the EU, it is contrary to the Treaties."[13]

10 www.dataprotection.ro, the webpages referred to were visited 1 February 2020.
11 Official Gazette no. 919 of 31 October 2018.
12 Official Gazette no.432 of 22 May 2018.
13 COM(2018) 43 final, p. 9.

8 The Decision of the Romanian Constitutional Court (hereinafter "RCC") no. 498/2018 regarding the exception of unconstitutionality of the provisions of art. 30 paragraphs (2) and (3), as well as the phrase "system of the electronic patient health file" in art. 280 paragraph (2) of Law no. 95/2006 regarding the health reform[14]

This Decision falls within the same context of ensuring coherence in the processing of personal data.

According to the principles set out in the RCC Decision, "if the state has instituted, by law, a measure in the application of the right to protection of the person's health, still the state has the obligation to protect and guarantee the confidentiality of the medical information processed, by a normative act of the same level, respectively by law. Thus, from this point of view, the positive obligations associated with the two rights are correlative and interdependent, and there must be a fair balance between them. The state is not allowed to protect a constitutional right, to the detriment of the other right, also protected, because it could reach the situation where the latter's affectation is so strong that the initial advantage obtained appears as being insignificant in this equation. Therefore, at normative level, complementarity and proportionality must characterize the relationship between the two constitutional rights".

Question 2

Article 26 of the Romanian Constitution states in paragraph 1, that: "The public authorities respect and protect the intimate, family and private life". The provisions of Regulation (EU) 2016/679 apply directly regarding the processing of the personal data of the people concerned.

According to the case law of the RCC, the right to intimate family and private life includes the right to the protection of personal data. In this regard, we mention the Decision of the Constitutional Court no. 498/2018 regarding the exception of unconstitutionality of the provisions of art. 30 paragraphs (2) and (3), as well as the phrase "system of the electronic patient health file" contained in art. 280 paragraph (2) of Law no. 95/2006 regarding the health reform.[15]

14 Official Gazette no. 650 of 26 July 2018.
15 Official Gazette no. 650 of 26 July 2018.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Article 5 GDPR contains directly applicable provisions on the principles of processing personal data, including the "purpose limitation" and "data minimisation" principles.

The data controller is responsible for compliance with the processing principles and must be able to demonstrate that compliance.

Question 4

Litigations concerning the application of the GDPR are at the beginning.

Question 5

The processing of personal data in a digital context has not been widely debated at national level.

Question 6

Decision no. 174/2018 regarding the list of operations for which the impact assessment on the protection of personal data is mandatory provides, inter alia, that "for the processing of personal data in order to carry out a systematic and comprehensive assessment of personal aspects relating to natural persons, which is based on automatic processing, including the creation of profiles, and which grounds decisions that produce legal effects on the individual or that affect it similarly to a significant extent", it is mandatory to assess the impact on the protection of personal data by the operators.[16]

By way of exception to the above, "impact assessment on data protection is not mandatory when processing under article 6(1)(c) or (e) of the GDPR has a legal basis in Union or domestic law, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of the respective regulatory acts."

Article 3 of Law no. 190/2018 establishes the following: the processing of genetic, biometric or health data, in order to carry out an automated decision-making process or

16 Official Gazette no. 919 of 31 October 2018.

for the creation of profiles, is allowed with the explicit consent of the data subject or, if processing is carried out on the basis of express legal provisions, with the establishment of appropriate measures to protect the rights, freedoms and legitimate interests of the data subject.

Question 7

The provisions of article 17 of the GDPR on the right to delete data ("right to be forgotten") are directly applicable. We specify that, according to article 55(3) GDPR, the National Supervisory Authority is not competent to supervise the processing operations of the courts acting in the exercise of their judicial function.

Question 8

Article 7 of Law no. 190/2018 on the implementation of the GDPR provides for rules on the processing of personal data for journalistic purposes or for purposes of academic, artistic or literary expression. It reads: "In order to ensure a balance between the right to the protection of personal data, freedom of expression and the right to information, processing for journalistic purposes or for the purpose of academic, artistic or literary expression may be made if it concerns personal data that were made public manifestly by the person concerned or closely related to the public personality of the person concerned or to the public interest of the facts in which he/she is involved, by way of derogation from the following chapters of the General Data Protection Regulation:

a. chapter II – Principles;
b. chapter III - The rights of the person concerned;
c. chapter IV - The operator and the person empowered by the operator;
d. Chapter V - Transfers of personal data to third countries or international organisations;
e. Chapter VI - Independent supervisory authorities;
f. Chapter VII - Cooperation and coherence;
g. Chapter VIII - Provisions relating to specific processing situations."

C Domestic Enforcement of Data Protection Law

Question 9

The National Supervisory Authority for Personal Data Processing aims at defending the fundamental rights and freedoms of natural persons, in particular the right to privacy,

family and private life, in connection with the processing of personal data and the free movement of such data.

The duties of the National Supervisory Authority are regulated by the GDPR and Law no. 363/2018 on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating criminal offenses or punishments, educational and safety measures and the free movement of such data.[17]

The National Supervisory Authority is headed by a president who is assisted by a vice-president in this activity. The president and vice-president of the National Supervisory Authority are appointed by the Senate for a period of five years. The term of office of the president and the vice-President can be renewed once. The procedure for appointing the president and the vice-president is provided in Chapter II of Law no. 102/2005, republished, and in Chapter IV of the same act, there are provisions regulating the staff of the Authority.

By Law no. 102/2005, the monitoring and control competences and duties of the National Supervisory Authority are ensured in accordance with the provisions of art. 55-59 of the GDPR.

Thus, the main duties of the National Supervisory Authority and its President have been established in national law, in line with the innovations brought about by the GDPR and Directive (EU) 2016/680. The independence and autonomy of the National Authority Supervision have also been strengthened in accordance with the provisions of article 52 of the GDPR.

In fulfilling the duties established by articles 57 and 58 of the GDPR, a new chapter, entitled "Exercising the powers of control and solving complaints" was introduced in Law no. 102/2005, which establishes in detail, the procedures for handling investigations and complaints.

At the same time, the main contravention sanctions, namely the warning and the fine, as well as the corrective measure of the type of admonition, were established, taking account of the new corrective measures that the National Supervisory Authority can take in line with article 58, para. 2 of the GDPR.

In addition, the GDPR establishes in what way the measures ordered by the National Supervisory Authorities can be challenged, both by the operators and by the people concerned, in accordance with the tasks assigned to the Member State under articles 58(4) and (5).

17 Official Gazette no. 13 of 7 January 2019.

Question 10

According to Decision no. 133/2018 regarding the approval of the Procedure for receiving and solving complaints:[18]

- complaints may be filed by any person concerned, especially if his or her habitual residence or place of work is in Romania or where the alleged violation has occurred on Romanian territory;
- complaints may be filed at the headquarters of the Supervisory Authority or sent by post, including electronic mail, or by using the electronic complaint form available on the institution's website;[19]
- complaints may be filed personally or through a representative, including through a non-patrimonial organisation active in the protection of their personal data;
- petitioners shall be informed in writing of the admission of the complaint, including whether they have undertaken a more thorough investigation or coordination with other supervisory authorities, and of the evolution or outcome of the investigation
- the person concerned dissatisfied with the way of solving his complaint may appeal to the administrative court of the competent tribunal after scouring the preliminary procedure provided by the Law on administrative contentious no. 554/2004, with subsequent amendments and completions.

Question 11

In addition to those mentioned in answer 9, Law no. 190/2018 on the implementation of the GDPR[20] establishes the derogatory sanction regime, including pecuniary sanctions, applicable to public authorities and bodies, giving priority to the prevention mechanism, before the application of the fines.

Question 12

From the information held, prior to the application of the GDPR, one person has been awarded moral damages in one litigation.

18 Official Gazette no. 600 of 13 July 2018.
19 www.dataprotection.ro.
20 Official Gazette no. 651 of 26 July 2108.

Question 13

According to the provisions of article 20 of Law no. 102/2005, republished, any person concerned who considers that the processing of her personal data violates the legal provisions in force has the right to file a complaint to the National Supervisory Authority, especially if her habitual residence or place of work is in Romania or where the alleged violation has occurred on Romanian territory.

The complaint must be submitted personally or by a representative, with the attachment of the mandate issued under the law by a lawyer or of a notary proxy, as the case may be. The complaint may also be filed by the person's representative who is a spouse or a relative up to the second degree including.

If the complaint is filed through a body, organisation, association, or foundation without a patrimonial purpose, they must prove that they have been legally constituted, with a statute providing for public interest objectives, and that they are active in the field of the protection of the rights and freedoms of data subjects with regard to the protection of personal data. In this case, the complaint shall also include the mandate or the notarial proxy, as the case may be, in which the limits of the mandate given by the person concerned shall be indicated.

Question 14

The GDPR establishes a new mechanism for cooperation between national supervisory authorities involving a European body with legal personality - the European Data Protection Board (EDPB). It is responsible for mediating positions between national supervisors, as well as for developing guidelines and recommendations for its unitary application across the European Union.

The Authority also cooperates at national level with other public authorities and institutions in the effective application of the legislation on the protection of personal data.

D Data Processing for National Security Purposes

Question 15

Law no. 51/1991 on the national security of Romania, republished[21], defines in article 1 the phrase "national security" as follows: "The national security of Romania means the

21 Official Gazette no. 190 of 18 March 2014.

state of legality, equilibrium and social, economic and political stability necessary for the existence and development of the Romanian national state as a sovereign, unitary, independent and indivisible state, the maintenance of the rule of law as well as the climate of unhindered exercise of the fundamental rights, freedoms and duties of citizens, according to the democratic principles and regulations established by the Constitution."

Slovakia

Lilla Garayova[*]

A Setting the Scene

Question 1

On 30 January 2018, a new act on the protection of personal data in the Slovak Republic was published in the Collection of Laws under the number 18/2018 Coll. The New Personal Data Protection Act replaced the former Act No. 122/2013 Coll. on the protection of personal data. The reason for the adoption of the New Personal Data Protection Act was primarily due to the European reform of the law on the protection of personal data, implemented in particular by the General Data Protection Regulation (hereinafter "GDPR")[1]. The New Personal Data Protection Act entered into force alongside the GDPR on 25 May 2018. The Act largely duplicated the provisions of the Regulation, while transposing the so-called "Police Directive" or "Law Enforcement Directive" (Directive (EU) No 2016/680, hereinafter "LED") into the Slovak legal order at the same time. The new national legislation mirrors the provisions of the regulation, and in some cases is in stark contrast with the 2013 national legislation.[2] The main differences include expanding the range of traditional personal data (name and surname) to include new types of data such as IP addresses or cookies.

The structure of the national legal framework of the Slovak Republic is as follows below.

Main Act
Data Protection Act No. 18/2018 Coll;[3]

---

* PhD, Pan-European University, Faculty of International and European Law, Bratislava (Slovakia).

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

3 Act No. 18/2018 Coll. on Personal data protection and amendments and supplements to certain Acts.

Other relevant law

The Decree of the Office for Personal Data Protection No. 158/2018 Coll. on Data Protection Impact Assessment Procedure;[4]

Relevant ordinances/Other guidelines

List of processing operations subject to impact assessment (so-called Black List):[5]

- Legal processing of personal data related to clinical testing[6]
- Methodology compliance of personal data processing at schools[7]
- Guideline No. 2/2018 – legality of processing. Updated version as of 22 January 2019[8]
- Frequently asked questions related to photography and audiovisual records[9]
- Statement of the Data Protection Office of the Slovak Republic related to delivery writings in an administrative proceeding and administrative file inspection[10]

The Office for Personal Data Protection of the Slovak Republic is a state administration body with national jurisdiction over the territory of the Slovak Republic, that participates in the protection of fundamental rights of natural persons in relation to processing of personal data and executes data protection supervision, including supervision of personal data protection by competent authorities for performance of the task for the purposes of criminal proceedings.[11] The Office, when exercising its jurisdiction, acts independently and is governed by the Constitution of the Slovak Republic, constitutional acts, acts, other generally binding legal regulations and international treaties binding upon the Slovak Republic. The Office monitors the implementation of the Data Protection Act, as well as comments on drafts of Acts and drafts of generally binding regulations governing the processing of personal data.

4 The Decree of the Office for Personal Data Protection of the Slovak Republic of 29 May 2018 on the procedure for the assessment of data protection no. 158/2018 Coll.

5 List of processing operations subject to impact assessment on the protection of personal data of the Slovak Republic.

6 Legal processing of personal data related to clinical testing published by the Office for Personal Data Protection of the Slovak Republic.

7 Methodology compliance of personal data processing at schools published by the Office for Personal Data Protection of the Slovak Republic.

8 Guideline No. 2/2018 – legality of processing. Updated version as of 22 January 2019.

9 Frequently asked questions related to photography and audiovisual records published by the Office for Personal Data Protection of the Slovak Republic.

10 Statement of the Data Protection Office of the Slovak Republic related to delivery writings in an administrative proceeding and administrative file inspection.

11 https://dataprotection.gov.sk/uoou/en, visited 1 February 2020.

Question 2

Privacy and Data Protection, though connected, are commonly recognised all over the world as two separate rights. In Europe, they are considered vital components for a sustainable democracy.

The Constitution of the Slovak republic passed by the Slovak National Council on 1 September 1992 in its Section 2 – Fundamental Human Rights and Freedoms – outlines the right to respect for private life. The legislation on the protection of personal data at a national level prior to the GDPR was solely based on the fundamental rights and freedoms embodied in the Constitution of the Slovak Republic. Pursuant to its article 19(2) and (3) everyone has the right to protection against unauthorized interference in private and family life and to protection against unauthorized collection, publication, or other misuse of personal data. Article 16 of the Slovak Constitution states that the inviolability of the person and its privacy is guaranteed whereby we mean the inviolability of privacy in connection with the whole area of intimate personal life and not only in terms of protecting the home and what goes on behind the doors of our house or apartment.

The right to privacy, or as the Constitution of the Slovak republic states – the right to private and family life – as enshrined in the constitution is one of the fundamental human rights the country was built on. The notion of data protection originates from the right to privacy and while both are instrumental in preserving and promoting fundamental values and rights, there was no explicit mention of the right to data protection in the Constitution of the Slovak republic. For many years the right to respect for private life as declared in the Constitution of the Slovak republic, seemingly sufficed. However, justified concerns on personal data breaches were not consistently considered as a violation of this right.

A broader interpretation of this right occurred in 2013, with the enactment of Act No. 122/2013 Coll. on the Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. which regulated the protection of rights of natural persons against wrongful interference with their private life in connection with the processing of their personal data. Moreover, it defined the rights, duties and liabilities in connection with personal data processing, as well as it established and outlined the scope of the powers and the organization of the Office for Personal Data Protection of the Slovak Republic.

On 30th January 2018, a new act on the protection of personal data in the Slovak Republic was published in the Collection of Laws under the number 18/2018 Coll. The New Personal Data Protection Act replaced the former Act No. 122/2013 Coll. on the protection of personal data. The reason for the adoption of the New Personal Data Protection Act was primarily due to the European reform of the law on the protection of personal data, most importantly the GDPR. The New Personal Data Protection Act entered

into force alongside the GDPR on 25 May 2018. The Act largely duplicated the provisions of the Regulation, while transposing the LED into the Slovak legal order at the same time.

The new national legislation mirrors the provisions of the regulation, and in some cases is in stark contrast with the 2013 national legislation. The main differences include expanding the range of traditional personal data (name and surname) to include new types of data such as IP addresses or cookies.

The new legislation tightens the requirements for consent to the processing of personal data, which must be specific, free, informed and unambiguous. The new law no longer regulates the obligation to prepare a security project, the obligation to keep records of the information system or the obligation to notify information systems to the Office for Personal Data Protection of the Slovak republic – all requirements under the former legislation. Instead, it introduces an obligation to keep records of processing activities (in particular employers employing at least 250 employees). Assessing the impact of processing operations on the protection of personal data, is virtually very difficult to understand or estimate at this point to the full extent. The new law introduces the right of data subjects to request the transfer of personal data in a structured form from one controller to another (e.g. via API or data archive). In contrast with the old legislation, the possibilities of processing personal data of children under 16 years of age – which requires the consent of the legal guardian – are significantly restricted. The new national legislation introduces the obligation to establish a data protection officer (instead of the previously existing voluntary authorization) in cases provided by law.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The current national legislation pursuant to the GDPR requires that all personal data processing should occur in a fair and lawful manner, for a specified and legitimate purpose, while only processing the data necessary to fulfil this purpose. The official guidelines of the Slovak National Supervisory Authority (hereinafter "NSA") – the Office for Personal Data Protection of the Slovak republic conclude that data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy. This includes data that is relevant, adequate and limited to what is necessary for the purposes for which they are processed.

The principle of fair processing primarily governs the relationship between the data subject and the controller. According to the current legislation controllers should notify the relevant data subjects, as well as the general public, that they will process data in a

transparent and lawful way. They are also obliged to demonstrate the compliance of processing operations with national legislation and the GDPR. Furthermore, controllers must act in a manner that best complies with the wishes of the data subject, especially in cases where their consent provides the legal basis for data processing. Data subjects need to be aware of any potential risks.

When it comes to the principle of fair processing, there is a case that needs to be highlighted. In *K.H and others v. Slovakia* the applicants, eight women – all members of the Roma community in Slovakia – received gynecological and obstetric treatment in eastern Slovakia.[12] After the treatment, none of them were able to conceive a child despite repeated attempts. The applicants recalled being asked to sign documents prior to their discharge from the hospital, but they were unable to identify the contents of the documents they signed. The eight women consented to representation by lawyers from the Centre for Civil and Human Rights, but in 2002, the Ministry of Health interpreted "legal representative" under the Health Care Act 1994 to mean only parents of underage children or as representatives of those whose legal capacity has been limited and therefore denied the attorneys access to view and photocopy the medical records. After suing the hospitals in 2002, the national courts found that the hospitals should permit the applicants to consult and make handwritten excerpts of the medical records, however found no right to photocopy of one's own medical records – allegedly to prevent the abuse of personal data – and no violation of rights protected under the Constitution or the European Convention of Human Rights (hereinafter "ECHR"). The Applicants took their case to the European Court of Human Rights (hereinafter "ECtHR"). In determining the scope of state obligations under article 8 of the ECHR (right to private and family life), the Court found that this right must be practical and effective and therefore access to files containing one's personal data must be allowed. The Court also found that the cost and arrangements for making the photocopies would have be borne by the individual making the request and the facility must present compelling reasons for refusing to provide copies. In this case the national courts justified prohibiting the applicants from making copies of their own medical records primarily on the need to protect relevant information from abuse. However, the ECtHR failed to see how the applicants could have abused information concerning themselves.[13]

While this case is another in a series of pronouncements from various human rights bodies, that have been increasing the pressure on Central and Eastern European governments to end the active discrimination against Roma peoples, especially women, in their countries; it is also incredibly significant from a data protection perspective. The ruling gives valuable insight to the interpretation of the principle of fair processing. According to the Court it is for the file holder to determine the arrangements for copying

12 ECtHR, *K.H. and others v. Slovakia*, 28 April 2009, App. No. 32881/04.

13 ECHR 2009/13 Case of *K.H. and others v. Slovakia*, 28 April 2009, App. No. 32881/04.

personal data files. However, data subjects should not be obliged to specifically justify a request to be provided with a copy of their personal data files. It is rather for the authorities to show that there are compelling reasons for refusing this.

Question 4

Legitimate interest is definitely the most flexible lawful basis for data processing, but the courts do not assume it is always the most appropriate. Relying on legitimate interests means taking on extra responsibility and can only be considered appropriate when using personal data in a way data subjects would reasonably expect and that would have a minimal privacy impact, or where there is a compelling justification for the processing. Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. Before opting to use legitimate interest as the basis of data processing, first the legitimate interest needs to be identified. Ensuing that, it needs to be demonstrated that the processing is necessary to achieve it, while balancing it against the individual's interests, rights and freedoms. If the same result can be achieved in another, less intrusive way, legitimate interest is no longer an option. There are cases, where there is a compelling justification for the processing and a more intrusive impact on the individual can be warranted – any potential impact needs to be justified. Legitimate interest is primarily considered in cases of fraud prevention and in cases of possible criminal acts or threats to public security.

Question 5

The question of personal data as "counter-performance" for provision of digital content came up in many debates on a national level, especially in debates concerning data actively vs. passively provisioned. Currently, Slovak legislation and legal practice draw a distinction between passive and active personal data provision. Simply put, the protection has only been applied so far, where the data subject had actively been providing data. Passive provisions include the use of cookies and IP addresses.

Even though article 6(1)(a) GDPR outlines that both active and passive data require consent, in Slovak legislative practice they are treated differently. Preservation of the IP address in the operation log of a website from the point of view of the regulation of personal data protection was not a problem in the prior application practice in Slovakia. To our knowledge and experience, this data has not been subject to regulatory review in the past,

based on annual reports from recent years.[14] However, with the effect of the GDPR, from May 2018 the processing of the IP address should be subject to increased privacy regulation. Traditionally in Slovakia, IP addresses have not normally been considered personal data, so it poses an interesting change in the application approach to consider passively provisioned data as personal data, which it undoubtedly is.

IP addresses can be labeled as personally identifiable in terms of privacy. Internet access providers and local network administrators can use appropriate means to identify Internet users to whom they have assigned IP addresses because they usually systematically "record" the file, the date, time, duration and dynamic IP address assigned to an Internet user. The same can be said for internet service providers who keep a traffic log on an HTTP server.

In particular, when IP addresses are processed to identify computer users (e.g. copyright owners who want to prosecute computer users for intellectual property infringement), it is expected that resources will be available that are reasonably likely to be used to identify persons, e.g. through a court subpoena – otherwise the collection of information would be of no importance – and therefore such information should be considered as personal data.

A specific case would be certain types of IP addresses that in certain circumstances do not reliably allow the user to be identified for various technical and organizational reasons. One example would be IP addresses assigned to a computer in an Internet cafe where no customer identification is required. It could be argued that the data collected on the use of a certain computer within a certain timeframe does not allow the user to be identified by appropriate means and therefore is not personal data. However, it should be noted that internet service providers are unlikely to know whether or not the IP address in question is an identifying address and therefore process the data associated with that IP address in the same way that they process the information associated with the IP addresses of users who are properly registered and identifiable. If the internet service provider is unable to distinguish with absolute certainty whether the data corresponds to users who cannot be identified, it will therefore have to process all IP information as personal data just to be on the safe side.

In general, an IP address can be defined as a unique identifier for a device connected to the Internet or local network. The IP address allows the systems to recognize other systems connected via the Internet protocol. For the sake of applicational clarity, it is necessary to note the concepts and differences between a static IP address and a dynamic IP address.

A static IP address is an address that is permanently assigned to a specific device by the ISP for the entire duration of the related contractual relationship and does not change

14 Annual privacy report published by the Office for Personal Data Protection of the Slovak Republic, years 2003-2018.

even when you restart the computer. A dynamic IP address is automatically assigned to your device by the internet service provider essentially every time the computer or router is powered on again using the Dynamic Host Configuration Protocol. It is controllable and allows the administrator to identify the device, either directly or indirectly, which can lead to the device user being identified. The ongoing debates resulted in legal guidelines on when IP address should be considered as personal data.[15] Based on these guidelines an IP address is personal data if it is processed by the internet service provider together with the identification (personal data) of the end user of the Internet connection. Static IP addresses used by individuals should be considered as protected personal data. The dynamic IP address that the online service provider maintains in relation to the data subject's browsing of its website content constitutes personal data for such service provider if it has the legal means to identify the data subject, also through other information held by the data provider's internet connection.

Based on new trends shifting the IP address to the level of personal data, this will need to be taken into account when formulating internal privacy policies, as well as taking security measures and describing them in the security documentation. This also needs to be taken into account in the legal information provided to the data subject on the website, in defining lists of personal data that are being processed, or in fulfilling other regulatory obligations. Alternatively, it will be necessary to mask (anonymise) the IP address so that it cannot be considered personal information.

Question 6

Yes, some legislative measures – albeit not comprehensive – were taken to restrict automated individual decision-making, which includes profiling. Companies are required to inform data subjects about the use of profiling and how to object to profiling. Data subjects have the right not to be subject to a decision.

Profiling and automated decision-making are used in an increasing number of sectors in Slovakia, both in the public and the private realm. To help decision-making, profiling is used in healthcare, taxation, banking, finance and marketing – among many other areas. Advancements in technology and artificial intelligence have made it easier to make automated decisions with the potential to impact the rights and freedoms of individuals. While automated decision-making has many commercial applications, and can result in increased efficiency and resource saving, it can pose significant risks when it comes to

15 The 30 steps of compliance with the new legislation on personal data protection published by the Office for Personal Data Protection of the Slovak Republic.

individual rights and freedoms, so the Slovak legislator is very clear about the need to use appropriate safeguards.

While Slovakia actively works on Artificial Intelligence strategies, to this date the government has not introduced a comprehensive document regulating the transparency and accountability of automated decision making. We have not found any examples of ethical frameworks being introduced and while the current legislation does introduce some safeguard measures on automated decision making, the current legal framework does not comprehensively describe the rights and obligations of citizens in this regard.

Algorithms used in software created for automated decision making are not subject to transparency and access to the algorithms or the source code which includes them is not possible, this is mostly due to copyright or security reasons. As an example, I would like to mention the Judiciary Council in Slovakia, using a tool for the random allocation of judges. In this case the software and the source code are owned by a third-party external company. While the security reasoning might be considered as valid, we must note that there are no external and independent audits set in place to monitor the fairness or the accuracy of the algorithmic operations.

Besides the lack of external audits, we have also not detected a single institution that would oversee or even possess comprehensive knowledge on which automated decision-making systems exist in Slovakia, meaning there is no public institution which is directly responsible for implementing policies and standards regarding algorithms used in automated decision-making in the public sector. The government should introduce ethical guidelines and legal policies to make sure that the system of algorithms is synergic. Obligatory audits should be performed by external independent entities.

The currently existing legal provisions together with the old-fashioned public administration system are not sufficiently responding to challenges connected with automated decision-making and profiling. The legal framework should describe the definition of automated decision making and profiling, keeping in mind the complex nature of these terms. Another key aspect that should be included in the legal framework is the guidelines on transparency of the source code of algorithms. Public institutions using algorithms in automated decision-making currently have no information on how these algorithms work, what data is processed and what factors are taken into account.

Question 7

One of the most striking additions introduced in the new GDPR, is the far stronger emphasis on the rights of the data subject, which includes the right to erasure (also known as 'the right to be forgotten'). A data subject can ask that their data be deleted in certain circumstances. This right is not absolute, it only arises in quite a narrow set of

circumstances. These circumstances are relatively limited, for example where the processing is based on consent, that consent is withdrawn and there are no other grounds for processing. Even where the right does arise, there are range of exemptions, for example where there is a legal obligation to retain the data. This means the right to erasure not only requires institutions to manage and control the purpose and consent of processing personal data for every individual, but it also contains provisions specifically referencing other regulations, which may overrule the right to be forgotten. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.[16]

The Slovak legal framework recognizes the right to erasure, especially in cases in which the personal data is no longer necessary for the purpose which it was originally collected or processed for; the lawful basis for holding the data was a consent – which has been withdrawn by the individual; the personal data was being processed for direct marketing purposes and the data subject objects to that processing; the personal data was processed unlawfully. Slovak legislation has specific provisions to protect the personal data of children. The right to erasure exists when the personal data processed was to offer information society services to a child. There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments. Therefore, if data collected from children is processed, particular weight should be given to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent. There are no legal provisions outlining how to make a valid request for erasure. Therefore, an individual can make a request for erasure verbally or in writing.

When it comes to the reality however, to date, there have not been many cases at a national level post-GDPR. The cases to date have mostly involved search engine results but it is important to remember that the GDPR right to erasure is not limited to online information, nor to search engine results. It is also worth noting that data protection law is unlikely to be the only issue in right to be forgotten cases.

We can conclude that the rights and obligations stated in article 17 GDPR correspond to the provisions of the national legislation. However, an additional condition is that data subjects rights may be restricted on grounds of Slovak public policy or economic mobilization.

16 Article 17(3) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Question 8

Yes, the new Data Protection Act of 2018 stipulates in article 78 that personal information may be processed without a data subject's consent for journalistic, academic, artistic and literary purposes. However, such processing must not breach a data subject's right to personality protection and privacy. According to article 78(1) Act No. 18/2018 the controller shall process personal data without the consent of the data subject, if the processing of personal data is necessary for academic purposes, for artistic purposes or for literary purposes; this does not apply if the processing of personal data violates the right of the data subject to protect his personality or the right to privacy or the processing of personal data without the consent of the data subject is excluded by a special law. Section (2) of the same act outlines processing personal data for the purposes of informing the public. The controller may process personal data without consent of data subject where this processing is necessary to inform the public by mass media means and where the personal data are processed by a controller based on its field of activity; this shall not apply where controller, by processing for that purpose, violates the right of data subject to the protection of his or her person or the right to privacy, or where such processing without consent of data subject is excluded by a special regulation or an international treaty binding upon the Slovak Republic.

The provisions above have more depth than it might seem at first glance. Article 85 includes an obligation of balancing the freedom of expression as well as the freedom of information. This balancing must be done by legislative measures. This is exactly how it was created in the national legislation but reconciling the freedom of expression with the right to privacy is proving to be a difficult task in reality.

C Domestic Enforcement of Data Protection Law

Question 9

The Office for Personal Data Protection of the Slovak Republic was established on 1 September 2002 on the basis of Act No. 428/2002 Coll. on the protection of personal data. The establishment of the Office as a state administration body was conditioned mainly by the need for the existence of an institution with investigative and intervention powers in this field, which results from legally binding acts of international law. Another important attribute of the establishment of the Office is its independence from individual public administration bodies. In order for the Office to carry out its tasks as efficiently as possible, without undue influence from political or other entities, it is necessary to ensure the full independence of the Office in the performance of its activities. This requirement stems

from the ever-increasing pace of social and technological changes that have significantly influenced the way in which the processing and transmission of increasingly large amounts of personal data is conducted. Any natural or legal person shall have the right to apply to the Office in the event of uncertainty arising from the application of the legal provisions concerning the protection of personal data or from suspected breaches of his rights in the processing of his personal data.

The scope of powers and list of activities have changed throughout the years as the relevant legislation went through various stages of evolution. Currently, in the post-GDPR realm the Office is a state administration body with national jurisdiction over the territory of the Slovak Republic, that participates in the protection of fundamental rights of natural persons in relation to the processing of personal data and executes data protection supervision, including supervision of personal data protection by competent authorities for the performance of the task for the purposes of criminal proceedings. The Office, when exercising its jurisdiction, acts independently and is governed by Constitution of the Slovak Republic, constitutional acts, acts, other generally binding legal regulations and international treaties binding upon the Slovak Republic. The headquarters of the Office are in Bratislava. The Office is a budgetary organisation.

The Office is headed by the president, who is elected and recalled by the National Council of the Slovak Republic upon proposal of the Government of the Slovak Republic. The term of office of the president is five years. The current president of the Office is Ms Soňa Pőtheová, who was elected by the National Council of the Slovak Republic on 14th May 2015. The president of the Office shall be represented by the vice-president of the Office, who shall be elected and recalled by the Government of Slovak Republic upon proposal by the president of the Office. The function term of office of the vice-president is five years. The vice-president is Ms Anna Vitteková, who was elected by the Government of Slovak Republic on 2nd December 2015 and with effect from 2nd January 2016.

The main tasks of the Office include:

1. Monitoring the implementation of the Data Protection Act;
2. Commenting on drafts of Acts and drafts of generally binding regulations governing the processing of personal data;
3. Providing consultation in the area of the protection of personal data;
4. Providing methodological guidelines on personal data processing to controllers and processors;
5. Promoting public awareness, in particular on risks and rights in relation to the processing of personal data;
6. Upon request, providing information to any data subject concerning the exercise of its rights under this Act and cooperating with supervisory authorities of other Member States for this purpose;

7. Verifying the lawfulness of processing of personal data by the competent authorities in exercising rights by a data subject pursuant to section 63 paragraph 5 and informing the data subject about the results of the verification within 30 days of the date of submission of the request for verification, or of the reasons why the verification was not carried out, and of the possibility to exercise the data subject's right to lodge a complaint to initiate proceedings pursuant to section 100 and for other types of legal protection pursuant to a specific regulation;
8. Monitoring development, in particular the development of information and communication technologies and commercial practices if they have any impact on the protection of personal data;
9. Cooperating with the European Data Protection Board in the area of personal data protection;
10. Submitting an annual report to the National Council of the Slovak Republic on the state of the protection of personal data at least once a year; the report on the state of personal data protection is published by the Office on its website and it is provided to the European Data Protection Board and to the Commission;
11. Cooperating with supervisory authorities of other member states, including the exchange of information, and providing them with mutual assistance in order to ensure a common approach to the protection of personal data under this Act and the special regulation.

To perform the aforementioned tasks, the Office is authorized

- to order the controller and the processor, or the representative of the controller or the processor if so authorised, to provide information essential for performance of its tasks;
- to obtain from the controller and the processor access to personal data and information that are necessary for the performance of its tasks; the provision of secrecy pursuant to special regulations remains unaffected;
- to enter the premises of the controller and the processor, as well as any equipment and means for processing personal data, to the extent necessary for the performance of his tasks, unless permission is required under a special regulation;
- to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions adopted pursuant to this Act or special regulations;
- to impose measures for liability, a fine pursuant to section 104 or an administrative fine pursuant to section 105 if the controller, processor, monitoring body or certification body infringes the provisions of this Act or special regulations;
- to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Act or special regulations;
- to order the controller or processor to bring processing operations into compliance in a specified manner and within a specified period with the provisions of this Act or special regulations;

- to order the controller to communicate a personal data breach to the data subject;
- to impose a temporary restriction or definitive restriction of personal data processing;
- to ask the controller or processor to give an explanation in case of suspicion of an infringement of an obligation under this Act, a special regulation or an international treaty binding upon by the Slovak Republic;
- to recommend the controller or processor to adopt measures for ensuring the protection of personal data in the filing systems;
- to order the suspension of data flows to a recipient in a third country or an international organisation.

Question 10

In Slovak legislation a complaint under the Act No. 9/2010 Coll. is considered to be a filing of a natural person or a legal person (complainant) seeking protection of his/her/its rights or legally protected interests he/she/it considers to have been infringed by the activity or inaction of a public authority, or pointing to specific deficiencies particularly infringements, the removal of which falls within the competence of the public authority.

The complaint shall be submitted:

- in writing, i.e. in a paper form;
- electronically with an authorization under a special regulation or sent through an access point that requires a successful authentication of the complainant; complaints made electronically without an authorization under the special regulation or sent not through an access point that requires a successful authentication of the complainant shall be confirmed within five working days by the complainant's own signature, by authorization under the special regulation or by sending the complaint through an access point that requires a successful authentication of the complainant.

According to the sec. 5 para. 2 and para. 3 of the Act No. 9/2010 Coll. the complaint shall contain:

- name, surname and residence address of the complainant or name, seat and name and surname of a person authorized to act on behalf of the complainant, if the complainant is a legal person;
- identification of the entity against which the complaint is addressed;
- indication of deficiencies referred to by the complainant;
- indication of claims of the complainant.

The Office for Personal Data Protection of the Slovak Republic shall handle the complaint within 60 working days. In cases the complaint is difficult to review, this period shall be

extended with a maximum of 30 days. The Office shall notify the complainant about the extension in writing. The complaint shall be deemed to have been settled by sending a written notification of the outcome of its review to the complainant.

According to the sec. 6 of the Act No. 9/2010 Coll. the Office shall postpone the complaint if:

- the complaint does not contain the required particulars;
- the subject of the complaint is or was reviewed by a court, law enforcement authority or is reviewed by another administrative authority;
- the complaint concerns a person different from the one who submitted it and an authorization is not enclosed;
- more than five years have passed from the event that is subject of the complaint as of the day when the complaint was delivered;
- the complaint is another repeated complaint;
- the complainant withdraws his/her/its complaint in writing or does not insist on its handling before the complaint is settled.

Question 11

In 2018 the Office for Personal Data Protection of the Slovak Republic has received 287 complaints, and as a result the Office lawfully imposed 38 fines totaling 132,600 euro for breaching personal data protection legislation. The average fine was 3,489 euro. The Office imposed the lowest fine of 500 euro for non-cooperation. The highest fine imposed was in the amount of 40,000 euro for a breach of the security of personal data processing.

Besides the standard requirements of the GDPR, the Slovak legislation has implemented additional sanctions, and it also empowers the Office to impose a fine of up to € 2,000 on persons who are not the controller or the processor for failure to cooperate with the Office. The Office may also fine the controller or the processor if they fail to ensure adequate conditions for the exercise of official controls under article 94 of the Slovak Data Protection Act.

The Slovak Data Protection Act recognizes only financial sanctions; however the Criminal Code sets out a criminal offence for the unlawful processing of personal data which was obtained under an obligation of confidentiality (punishable with up to 2 years of imprisonment).

Question 12

The concept of damages is not concisely defined in Act no. 40/1964 Coll The Civil Code as amended. This term has always been defined in several different ways. The broadest

notion of damages is: "(…) any harm which has been caused to someone or property (property or rights), except in the case of intangible harm."[17]

The scope for defining the concept of damages is greatly left to judicial practice. At present, the perception of damages in the narrower sense prevails, namely based on the judicial interpretation of article 422 of the Civil Code the courts acknowledge "any harm that occurred to the property of the injured party that is objectively expressible by the general equivalent, and is therefore remedied by the granting of property, in particular by the granting of money, unless there is a natural restitution."[18]

Slovak legislation has not historically awarded damages for intangible harm; any cases that might seem as compensation for intangible harm suffered, were in fact pecuniary damages only for the quantifiable monetary harm – cases of health injury for example do not include a pain and suffering, or a mental anguish component, damages are only paid to the amount of proven monetary harm – i.e. loss of earnings, medical costs.

Question 13

Article 80 of the GDPR introduces a collective action mechanism whereby not-for-profit bodies dedicated to personal data protection can initiate claims on behalf of data subjects whom allege their rights have been infringed. In theory, this provision should enhance the protection the GDPR affords to data subjects by giving authorised associations in each Member State the power to consolidate claims and represent them on a larger scale. The article has been welcomed by privacy campaigners in Slovakia. The reality is not as clear-cut as it might have seemed at first glance. Whilst the GDPR provides that data subjects "shall have the right to" initiate actions, it does not actually provide them with any actionable tool or procedural framework to kick-start the process.[19] It has left that particular task up to the individual Member States. As an EU Regulation, the GDPR has direct effect, and does not generally require transposition into Slovak law. Certain provisions give Member States flexibility however, and in Slovakia, the Data Protection Act 2018 legislates for the Slovak position in those areas. Article 80 is such a provision, the result being that the implementation of the class action mechanism is almost entirely at the discretion of the national legislature. The provision has mandatory and discretionary parts. In practical terms, the implementation of article 80 into Slovak legislation happened by publishing a set of guidelines providing a mechanism for data subjects to authorise third parties to make a complaint on their behalf. While NGOs, various organisations or associations have the right to lodge a complaint with the supervisory authority, it can only happen at the data

17 Act No. 40/1964 Coll. The Civil Code as amended.
18 Art. 422(1) of act No. 40/1964 Coll. The Civil Code as amended.
19 Art. 79(1) GDPR.

subject's instructions. The full impact of article 80 remains to be seen, but permitting qualified organisations and NGOs to initiate claims on behalf of data subjects with their mandate should now give ordinary litigants recourse to seek redress in circumstances where they would otherwise not have had the resources to do so.

Question 14

No, this trend is not yet visible in Slovakia. The only body acting on data processing related complaints is the NSA – The Office for Personal Data Protection of the Slovak Republic.

D Data Processing for National Security Purposes

Question 15

The only act relevant in this case would be Constitutional Act No. 227/2002 Coll. on State Security at the Time of War, State of War, State of Emergency, and State of Crisis. This Constitutional Act created legislative conditions for guaranteeing state security. According to the level and nature of threat or disturbance of the state security and on the basis of conditions laid down by the Constitution of the Slovak Republic and by this constitutional act, constitutional bodies can declare war, state of war, state of emergency or state of crisis in order to solve the crisis situation. There are also defined conditions and a scope of restriction of fundamental rights and liberties, as well as the extent of responsibilities at the time of the state of crisis. The constitutional act lays down also the method of performance of public authority at the time of war, state of war and state of emergency. The act itself does not define "national security" or even "state security". It does provide definition to a much broader term – security, and then goes on to mention the term national security in the ensuing articles.

Prior to April 2015, the Slovak data retention regime required providers of electronic communications to store indiscriminate traffic, localization data and data about the communicating parties, including unsuccessful calls, for a period of 6 months in the case of internet, email or VoIP communications or for a period of 12 months for other means of communication. In April 2015, the Grand Chamber of the Constitutional Court (PL. ÚS 10/2014)[20] effectively invalidated Slovakia's existing data retention regime, giving effect

20 Constitutional Court of the Slovak republic, Decision PL. ÚS 10/2014-78.

to *Digital Rights Ireland*.[21] The Constitutional Court proclaimed[22] provisions § 58(5) to (7) and § 63(6) of the Electronic Communications Act (Act No. 351/2011 Coll.), which until now required mobile network providers to track the communication of their users, as well as provisions of § 116 of the Penal Code (Act No. 301/2005 Coll.) and § 76(3) of the Police Force Act (Act No. 171/1993 Coll.), which allowed access to this data, to be in contradiction to the constitutionally guaranteed rights of citizens to privacy and personal data. As a consequence, these provisions lost their binding effect.

Following the Constitutional Court's 2015 decision, the government prepared a draft act that aims to enhance control over the data retention process and clearly details the situations in which data can be retained, stored and requested by state bodies. Specifically, the proposed law permits this only for the most serious crimes, such as terrorism or threats to the integrity of the country.

The new legislation is not in force yet. Under the current regime which consists of the parts of the old regime not invalidated by the Constitutional Court's ruling, traffic and location data must be destroyed or anonymized immediately after any communication has been finished. An exception to this is the retention of data that is necessary for invoicing a customer, however even this data can be stored only for the extent and duration justified by the practice of invoicing. Data retention, still regulated under the prior regime, is now only allowed if approved by a court order.

21 Judgment of 8 April 2014 in Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

22 Constitutional Court of the Slovak republic, Decision PL. ÚS 10/2014-78.

Slovenia

Nina Pekolj and Marjan Antončič[*]

A Setting the Scene

Question 1

At the time of submission of this report, Slovenia has not yet adopted a law to support or enable the implementation of the General Data Protection Regulation (hereinafter "GDPR"). The 2004 Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*, hereinafter "ZVOP-1") is formally still in force, being the third law governing personal data protection in Slovenia since 1990.[1]

With a single law, the new, fourth Personal Data Protection Act (hereinafter "ZVOP-2"), the Ministry of Justice, which is competent for the field of personal data protection, decided:

- To ensure the implementation of the GDPR provisions by defining, within the limits of the GDPR authorisation clauses, the national specifics of the personal data protection regime, thus preserving as much as possible the present high level of personal data protection in the Republic of Slovenia and the exercise of the human right to the protection of personal data (Article 38 of the Constitution of the Republic of Slovenia);[2] and
- To ensure the transposition of Directive (EU) 2016/680[3] into the legal order of the Republic of Slovenia, with the same goals.

---

* Nina Pekolj: Director of the Slovenian Agency for Data Protection Law, Slovenia. Marjan Antončič: Representative of the Slovenian Association for Electronic Identification and Electronic Trust Services.

1 The first Personal Data Protection Act of the Republic of Slovenia was adopted on 7 March 1990 (Official Gazette of the Republic of Slovenia, Nos. 8/90, 19/91 and 59/99 – ZVOP), the second Personal Data Protection Act was adopted on 8 July 1999 (Official Gazette RS, Nos. 59/99, 57/01, 59/01 – corr., 73/04 – ZUP-C and 86/04 – ZVOP), and the third Personal Data Protection Act on 15 July 2004 (Official Gazette RS, Nos. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 and 94/07 – official consolidated text; ZVOP-1).

2 *"The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.*
The collection, processing, designated use, supervision, and protection of the confidentiality of personal data shall be provided by law.
Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data."

3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

Question 2

Both rights were dealt with by the 2004 ZVOP-1, which provided in article 1: "*This act shall establish rights, obligations, principles and measures to prevent the unconstitutional, illegal and unjustified interference with the privacy and dignity of an individual in the processing of personal data*." The same approach is maintained by the draft ZVOP-2.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

ZVOP-1 is based on three principles of personal data protection: the principle of legality and fairness (article 2), the principle of proportionality (article 3) and the prohibition of discrimination (article 4).

Under article 2 of the ZVOP-1, **the principle of fairness** is a kind of general clause[4] requiring the bona fide and, above all, non-deceptive behaviour of data controllers. The breach of this principle has most often been detected by the national supervisory authority (i.e. the Information Commissioner) in situations where the controllers of personal data record the purpose(s) of the processing of personal data vaguely or in a way that allows for broad interpretation[5] (e.g., vaguely or incompletely written consent forms for the processing of personal data or ambiguous general terms and conditions of the controller[6]). Such actions by the controller may cause the individual to be mistaken in the belief that his or her personal data will be processed only for a specific purpose, but not for any other purpose, which constitutes an infringement of the provisions of the ZVOP-1, for which fines and reprimand are imposed.

On the other hand, the **principles of purpose limitation and data minimisation** were most commonly and narrowly interpreted by a national court (i.e. the Administrative Court; for instance, in the case of video surveillance in the home for older adults in 2015[7]).

---

penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

4 N. Pirc Musar et al, *Zakon o varstvu osebnih podatkov s komentarjem* [Personal Data Protection Act – A Commentary], Ljubljana, GV Založba 2006, p. 43.

5 Ibid, p. 43.

6 Information Commissioner, Opinion no. 092-4/2006/347, 15 June 2006.

7 The Administrative Court Judgment II U 195/2014 of 21 January 2015.

The principle of proportionality has been interpreted frequently by national courts, both by the Administrative Court[8] as well as the Constitutional Court. In several decisions, the latter has already decided on possible excessive interference with human rights and fundamental freedoms, and to this end has formulated, through its case law, the so-called strict proportionality test. This test involves assessing three aspects of the interference: a test of appropriateness, a test of necessity, and a test of proportionality in the narrow sense. Only if the interference passes all three aspects of the test can it be declared constitutionally permissible. One of the more notable cases was the Constitutional Court's decision,[9] in which it assessed the admissibility of the public disclosure of personal data in relation to past due and unpaid tax liability.

Although ZVOP-1 does not directly regulate **the data minimisation principle**, the latter was also respected in the case law. The Administrative Court repeatedly assessed the admissibility of the creation of new personal data filing systems based on personal data (lawfully) obtained from various publicly available official records (i.e. the business register). In doing so, it always stated that the fact that certain personal data in a particular personal data filing system are public does not mean that it is permitted for such personal data, together with personal data from other publicly available personal data filing systems and personal data from other publicly available sources, without explicit legal basis, are combined or used to create and maintain a new filing system that is, as such, made available to other users.[10]

Question 4

Still valid ZVOP-1 (*mutatis mutandis* maintained by the draft ZVOP-2[11]) separates the legal bases for processing personal data in the public sector from the legal bases in the private sector. Legislative provisions imply stricter rules for the processing of personal data by the public sector than the private sector since the legal bases are narrower.[12] **The public sector** must have a basis in law for any processing of personal data, and the processing of personal data based on personal consent or contract or for the exercise of legitimate powers, tasks or obligations of the public sector is permissible only exceptionally. Under the opinion of the Information Commissioner of the Republic of Slovenia,[13] it is

8 The Administrative Court Judgment I U 213/2016-16 of 17 May 2017.
9 The Constitutional Court Decision U-I-122/13 of 10 March 2016.
10 The Administrative Court Judgments I U 817/2016 of 6 March 2017 and U 2477/2005 of 10 October 2007.
11 Government of the Republic of Slovenia, EVA Proposal: 2018-2030-0045, Personal Data Protection Act, 6 March 2019.
12 Pirc Musar *et al*, 2006, p. 89.
13 Information Commissioner, Opinion No. 061-15/2005 of 13 January 2006.

also necessary to emphasise that pursuant to article 38(2) of the Slovenian Constitution, the "basis in the law" may be considered **exclusively law**, excluding by-laws.

Unlike the public sector, the processing of personal data in the private sector is most often performed based on **consent**, and it is also permissible for the controller's (from the private sector) **legitimate interests** to the extent that they clearly outweigh the interests of the data subject. In doing so, the Administrative Court interprets the legal standard "clearly" in such a way that they must be evident as such *prima facie*, without a detailed or in-depth weighing[14]. In the assessment of "legitimate interests", the Administrative Court, as a rule, referred to the more familiar test of proportionality, the content of which was clearly defined by the Constitutional Court. Thus, with reference to Opinion no. 06/2014 of the Article 29 Data Protection Working Party, relating to the notion of legitimate interests of the data controller, Administrative Court in its decision of 2016[15] decided that when applying the test of legitimate interests, it is necessary to assess:

1. The nature and source of the legitimate interests of the controller or persons to whom personal data have been provided; and
2. Whether processing is indispensable to the pursuit of those interests; and
3. The impact of such processing on the data subjects.

Although the GDPR has not yet been implemented in the national legislative framework by the time this report is being prepared, one can expect at least equally rigorous data protection arrangements requirement in the digital sphere. Already according to the old ZVOP-1, one should not deviate from the already established strict interpretation of the general fundamental principles of the law on personal data protection, despite the pressures and advances in information technology, which accelerates the processing of personal data of all types of activities. Only by restrictively interpreting the provisions of the ZVOP can we protect an individual from personal data abuse. As one can read in the commentary of the still valid ZVOP-1:

> "*One has to be mindful of the fact that information technology can conceal pitfalls that make it impossible for an individual to control all processing of personal data through his or her consent.*"[16]

Attention should also be drawn to the fact that, as an individual, the consumer cannot bring action against the recipient of a personal data (company) for its alleged unlawful conduct in a civil procedure at contractual level, since the control of respect for the law

14 The Administrative Court Judgment I U 1538/2015 of 7 July 2016.
15 Ibid.
16 Pirc Musar *et al*, 2006, pp. 89–90.

on the protection of personal data is left to the competent administrative authorities. Thus, the individual is left with only the possibility of enforcing contractual and compensation mechanisms.

Question 5

The national Consumer Protection Act (*Zakon o varstvu potrošnikov* – ZVPot)[17] regulates consumers' rights in the offering, selling and other marketing of goods and services by companies, including digital content stored on durable media. In addition, some provisions of the ZVPot also apply to contracts for the supply of digital content, which are not recorded on a tangible medium and are concluded at a distance or outside business premises. In practice, the latter can also have direct effects in the field of personal data protection or the right to privacy, even if the ZVPot does not cover the supply of personal data as a counter-charge (the so-called "purchase price").

As an example, the limitation of the right of withdrawal per Article 43č of the ZVPot is highlighted. Under article 43č of the ZVPot, the consumer has the possibility within 14 days from the date of conclusion of the contract to inform the company that he or she is withdrawing from the contract. Upon expiry of this period, unless otherwise expressly provided by the contract, the consumer loses this right. The only condition required by law to do so is the consumer's prior knowledge that, by entering into a contract, he loses the right to withdraw from the contract. However, the law does not stipulate that such consent must be provided actively. It is sufficient to include such provisions in the general, commercial conditions of business of the company, to which consumers do not pay attention in practice. However, in the opposite case, if the consumer would have been clearly and unequivocally aware, at the time of the conclusion of the contract, that by consent or by entering into a contract it loses the right of withdrawal, such a provision in a contract for the supply of digital content in exchange for the provision of personal data may constitute a violation of the fundamental principle of legality of the processing of personal data, since it is inherently contrary to the concept of free consent.

In one of its opinions[18], the Information Commissioner also expressed its position on specific aspects of digital content supply contracts. In the preliminary findings summarised below, the Information Commissioner thus stated that the actual aim of the latter is to

17 Official Gazette of the Republic of Slovenia, No. 98/04 – official consolidated text.

18 Information Commissioner, *Mnenje glede predloga Direktive Evropskega parlamenta in Sveta o nekaterih vidikih pogodb o dobavi digitalnih vsebin, COM (2015) 634 final [Opinion on the Proposal for a Directive of the European Parliament and of the Council on certain aspects of digital content supply contracts, COM (2015) 634 final]*, 18 April 2017, www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/MP_mnenje_o_predlogu_Direktive_o_nekaterih_vidikih_pogodb_o_dobavi_digitalnih_vsebin.pdf. All webpages referred to were visited on 23 August 2019.

legitimise the situation where an individual for the supply of a particular digital service, as a contrary fulfilment, actively provides more personal data than would be reasonably necessary to perform the contract. This essentially constitutes consent as the legal basis for the processing of personal data, while not all elements of the consent concept are respected. Consent is considered valid, among other things[19] given freely, so that the individual has the ability to influence what personal data he or she will provide and for what purpose the personal data will be processed (the so-called granularity or breakdown of the consent[20]), and not the other way around, as a "take it or leave it" package – a typical situation in delivering digital content.

For this reason, the Information Commissioner addressed to the Ministry of Justice to unambiguously define the legal basis in terms of the GDPR in the case of contrary fulfilment of the consumer for the supply of digital content by providing his or her personal data, and at the same time, to avoid the ambiguity and legal uncertainty by creating new bases and conditions for the processing of personal data or new terms (such as "other data", "active" provision of personal data, etc.), which do not exist within the data protection framework because this could result in a lower level of protection than the GDPR provides.

Question 6

The ZVOP-1 already contained provisions that conditionally allowed automated decision-making. Under article 15 of the ZVOP-1, automated decision-making that results in legal effects for an individual or significantly affects her is permissible provided that the decision is made during the conclusion or performance of the contract or if it is so provided by a statute, which also includes measures to protect the legitimate interests of the data subject (in particular, the possibility of a legal remedy against such a decision).

Article 44 of the draft ZVOP-2[21] provides for the automatic processing of personal data, including the creation of profiles, subject to the fact that such processing is expressly stipulated by law laying down measures for the protection of human rights and fundamental freedoms and legitimate interests of the individual, such as the right to personal intervention by the controller, to freedom of communication and to challenge the decision. Additionally, the draft ZVOP-2 also provides for a data protection impact assessment preliminary measure, but it is not entirely clear whether such impact assessment is required whenever

19 Other conditions introduced by the concept of consent are: the individual expresses it with an active action, it is given in advance and the individual has the option of withdrawing the consent.

20 Information Commissioner, *Consent*, www.ip-rs.si/legislation/reforma-european-legislative-framework-for-security-private-data/key-area-ordered/acceptance/#c1929.

21 Government of the RS, *EVA proposal: 2018-2030-0045, Zakon o varstvu osebnih podatkov*, 6 March 2019, www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/Mandat_2018-2022/Zakonodaja/ZVOP-2_6.3.19_splet.pdf.

automated decision-making procedures are introduced, or only in the case of processing specific types of personal data or even if there is a risk of discrimination[22]. The explanatory note to the draft ZVOP-2 reasons that:

> "*The focus of the impact assessment means that such assessment must also include an impact assessment on related human rights and fundamental freedoms, in particular on non-discrimination, but also on freedom of movement, universal privacy, dignity, communication privacy, etc.*"

One can assume that the same provision will *mutatis mutandis* apply also to automated decision-making and processing of personal data in the case of crime prevention, investigation, detection or prosecution.

Question 7

The valid ZVOP-1 distinguishes between the right of an individual to erase personal data under article 32(1) in cases where the individual proves that his or her personal data were collected or processed in breach of the law and between the right to request the termination of processing in cases where the latter is implemented without a proper legal basis. The individual exercises his or her right to erase the personal data, as well as the right to complete, correct and block, by **request**, which should be addressed to the data controller. The burden of proof that personal data is incomplete, inaccurate, not up-to-date, or collected or processed in violation of the law, lies with the individual.

However, the right to request the termination of the processing of personal data by **complaint** may only be invoked against the controller of the personal data where the controller from the public or private sector has no legal basis for the processing of personal data in the following cases:

- In the public sector: when the controller processes the personal data of an individual for the exercise of legitimate powers, tasks or obligations, but through this processing interferes with the legitimate interest of the data subject (infringement of article 9(4) of ZVOP-1);
- In the private sector: when the controller processes the personal data of an individual because it is necessary for the pursuit of the legitimate interests of the private sector,

22 Information Commissioner, *Predlog novega Zakona o varstvu osebnih podatkov (ZVOP-2) [Draft new Personal Data Protection Act (ZVOP-2)] – EVA: 2019-2030-0045 – OPINION*, 25 March 2019, www.ip-rs.si/fileadmin/user_upload/Pricomments_of_prescriptions_prescriptions__Pdf_in_doc_/ZVOP2_change_IP_marec2019_concni.pdf.

but these interests (obviously) do not outweigh the interests of the data subjects (infringement of article 10(3) of ZVOP-1).

It is also worth highlighting the differences in the enforcement of judicial protection. Pursuant to article 34 of the valid ZVOP-1, the following distinction applies[23]:

- If an individual seeks judicial protection because his or her rights have been infringed (and the infringement has not yet ceased), such protection shall be provided by the court in the administrative dispute procedure;
- If an individual seeks judicial protection when the infringement has already ceased, then, as a rule, he or she shall assert his or her rights in civil litigation (e.g. a claim for damages) and only exceptionally in an administrative dispute (e.g. a declaratory claim for the existence of the infringement).

However, without any distinction, both the administrative dispute and the civil procedure are considered urgent and priority, which in practice means as soon as possible, since a judicial protection of fundamental human rights as guaranteed by the Constitution is at stake.[24]

According to the Ministry of Justice's systematic explanations,[25] which are non-binding but clearly indicate which provisions of the ZVOP-1 are still (meaningfully) applicable from the date of entry into force and direct application of the GDPR and, in accordance with the opinion of the Information Commissioner, presented below, new legislation may be expected, which will implement the GDPR into national law, the right to erasure or regulate the right to cease processing of personal data differently. The systematic explanations indicate that provisions mentioned above are no longer applicable, except for the provisions on the judicial protection of individual rights.

Recently, the Information Commissioner also issued an opinion, taking into account the GDPR provisions,[26] explaining that the right to the erasure of personal data is justified only in cases where there is no legal basis for the processing of personal data. If the controller processes personal data lawfully or for the performance of a task in the public interest or for the exercise of public authority that has been assigned to the controller or needs personal data to exercise the right to freedom of expression and information, or if there is a legal

23 N. Pirc Musar *et al*, 2006, p. 270.

24 Ibid, p. 272.

25 Ministry of Justice, *Prva sistemska pojasnila Ministrstva za pravosodje ob začetku razvoja uporabe nove evropske zakonodaje o varstvu osebnih podatkov, prva inačica [The first systemic explanations by the Ministry of Justice commencing the developement of the application of the new European legislation on personal data protection, version one]*, 28 May 2018, www.mp.gov.si/en/media_center/news/7568/.

26 Information Commissioner, *Umik zaključnega dela [Withdrawal of Final Work], No. 0712-1/2019/1534*, GDPR Opinion Search Engine, 24 June 2019, www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=703.

basis for the processing of personal data, then erasure cannot be justified. In such a case, the conditions and retention periods laid down by the legislation for individual documentary material must be respected. In accordance with Article 17 of the GDPR, the Information Commissioner has taken the view that the right to erasure is not absolute[27] and that prior to any request for erasure, the controller must thoroughly verify that the erasure is justified and, consequently, whether erasure of personal data is a valid act of the controller. If the controller determines that a basis for data retention no longer exists, the request for erasure must be granted, since the content of the data may no longer be retained, but evidence of deletion without the content of the data may be retained.

Question 8

In Slovenian national law, the right to privacy and the right to freedom of expression and information are human rights, which are in conflict in the weighing of interests and are thus restrictively interfered with[28]. Those two rights mentioned above are not absolute and are not unlimited. A proper boundary between the two must be found following the constitutional principle of proportionality.[29]

The right to freedom of expression is multifaceted and includes, in addition to the right to disseminate, the right to receive opinions and information. Freedom of expression is one of the underlying conditions for the functioning of democratic rule since in a democratic society, it is necessary to allow the circulation of information and opinions. The Constitutional Court of the Republic of Slovenia stated in one of its decisions (*Up-106/01*) that the right to freedom of expression helps to form an impartially informed public, determines its ability to control all branches of government and ensures the effective functioning of political opposition to the respective authorities. However, restrictions on the right to freedom of expression and information are not always the same. Above all, the position of the media in relation to the state and to the individual must be distinguished. The state is in a superior position, so media rights are less restricted. Examples of permissible restrictions are only the measures provided for by law, which are necessary in a democratic society for the sake of the national security, the fight against terrorism, the

27 Information Commissioner, *Pravica do pozabe, Rok hrambe OP [Right to be forgotten, personal data retention period]*, No. 0712-1/2019/1463, GDPR Opinions Search Engine, 14 June 2019, www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=719.

28 R. Čeferin, Meje svobode tiska, *Analiza sodne prakse Ustavnega sodišča Republike Slovenije in Evropskega sodišča za človekove pravice [The Limits of Freedom of the Press, Analysis of the Case Law of the Constitutional Court of the Republic of Slovenia and the European Court of Human Rights]*, GV Založba, Ljubljana, 2013, p. 55.

29 Pirc Musar et al, 2006, p. 136.

prevention of disorder or crime, the protection of health or morals, the protection of confidential information or the protection of the authority and impartiality of the judiciary.[30]

In contrast, media rights are more limited when it comes to the protection of the individual. In doing so, the case law has drawn a distinction between individuals who are "ordinary citizens" and individuals who are "public figures". The latter are also subject to the distinction between the absolute and relative public figures. The requirement to respect privacy is automatically reduced in proportion to the amount of an individual's own entering into the public life, and their personal information is, in principle, allowed to be published without the consent of that person. The absolute public figures are those who are constantly under the scrutiny of the public due to their role and function in society (e.g. politicians, entertainers and other artists, top athletes, officials, etc.). Relative public figures are those persons who are of interest to the public only temporarily because of their connection with a particular event (e.g. winners of various competitions or events, lot winners, perpetrators of serious crimes and others). Information on relative public figures is allowed to be published only when they are of interest to the public due to the event and not later.[31]

Restrictions on the right to freedom of expression due to the protection of the right to privacy are also laid down in the Media Act. According to Article 45 of the Media Act, the media are thus not entitled to information if it would violate the confidentiality of personal data under the law unless their publication can prevent a serious crime or imminent danger to the lives and property of people.[32] In this way, the Media Act confirms the established case law, which was formed before it was drafted.[33]

On the other hand, case law has been established, according to which the right to freedom of expression outweighs the right to privacy in the case of public interest. In its decision No. Up-2940/07, the Constitutional Court took the view that, in all the circumstances of the case, the journalist was entitled to disclose in the public interest the name and surname of the suspected police station commander. The Constitutional Court also expressed similar position in the decision Up-570/09, in which it adjudicated that a journalist was entitled to publish the full name of a known entrepreneur, who deposited money in his bank account in a suspicious manner, since the public has the right to be informed of irregularities or breaches of the anti-money laundering regulations of the bank.[34]

30 L. Koman Perenič, *Informacijski pooblaščenec, Varstvo osebnih podatkov in mediji [Information Commissioner, Personal data protection and media]*, 26 May 2009, www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/OP_in_mediji.pdf.

31 Ibid.

32 Ibid, p. 19.

33 The Higher Court in Ljubljana Judgment II CP 476/99, 28 September 2000.

34 R. Čeferin, 2013, pp. 55–57.

Following the latest version of the draft ZVOP-2[35], restrictions on the right to freedom of expression are set in such a way that to exercise freedom of expression, it is permissible to use, publish or otherwise disclose personal information under the following conditions:

1. If the individual has consented to the use, publication or disclosure,
2. If the individual has already disclosed or made available the personal data (exercise of the right to information self-determination),
3. If the personal data have already been lawfully made available to the public,
4. If the personal data were obtained on the basis of the presence of the individual in public places (e.g. public gathering) or events where, in all circumstances, the individual cannot reasonably expect privacy protection and in a manner that does not significantly interfere with reasonably expected privacy (reasonable expectation of privacy concept),
5. In the case of the lawful publication of an opinion or valuation, where the publication of personal data in their context is necessary to justify the opinion or valuation,
6. If the personal data have been obtained in another lawful manner,
7. If the public interest in informing the public, the right to be informed and freedom of expression outweighs the legitimate interests of protecting the privacy and other personal rights of the individual, or
8. If so provided by another law (e.g. State Prosecution Service Act).

At the time of drafting this report, it was not possible to determine how and to what extent the new legislation will regulate the subject area or how much it will deviate from the established case law. Nor can it be stated how the new legislation will regulate the conflict of privacy with the right to freedom of expression and information for academic, artistic or literary expression, and not solely for journalistic purposes.

C Domestic Enforcement of Data Protection Law

Question 9

Information Commissioner of the Republic of Slovenia

The national supervisory authority is called the Information Commissioner of the Republic of Slovenia. Its official website[36] states that the Information Commissioner is an autonomous and independent body established on 31 December 2005 with the Information

35 Government of the RS, *EVA proposal: 2018-2030-0045, Zakon o varstvu osebnih podatkov*, 6 March 2019, pp. 143–144, www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/Mandat_2018-2022/Zakonodaja/ZVOP-2_6.3.19_splet.pdf.

36 Information Commissioner, *Pristojnosti [Powers]*, https://www.ip-rs.si/en/about/competences/.

Commissioner Act (ZInfP). The body supervises both the protection of personal data, as well as access to public information. The Information Commissioner has the status of an autonomous and independent state body.

Judicial protection

There is no appeal against the decision or order issued in the inspection procedure, which is kept as an administrative procedure with the Information Commissioner. An administrative dispute is allowed before the Administrative Court of the Republic of Slovenia, which is primarily intended to resolve disputes between the affected individuals and the authorities. This is a *sui generis* administrative dispute pursuant to Article 34 of ZVOP-1, which, as reasoned in one of the decisions by the Supreme Court of the Republic of Slovenia substantially represents an upgrade of protection under ZUS-1, since it provides adequate judicial protection when it comes to the authoritative action of the authorities in case of infringement of the rights guaranteed by the ZVOP-1. In doing so, by ZVOP-1 in conjunction with ZUS-1, the legislator provided a unique form of judicial protection of the right to the protection of personal data (Article 38 of the Constitution), also as a specific justification of the broader right to privacy (Article 35 of the Constitution), which consequently excludes the need for subsidiary judicial protection of constitutional rights pursuant to the Article 4(1) of ZUS-1[37].

Human Rights Ombudsman

Pursuant to Article 59 of ZVOP-1, the protection of personal data also falls within the competence of the Human Rights Ombudsman. The Ombudsman, also as the Information Commissioner RS, acts as a fully independent and autonomous body, but unlike the Information Commissioner RS, the Ombudsman does not have any leverage for coercion in cases where his opinions are not respected, or action upon them is not taken. The Ombudsman also performs his duties in the field of personal data protection exclusively in relation to state bodies, bodies of local self-governing communities and holders of public authority. Unlike the Information Commissioner RS, as a result, the Ombudsman has no real power to interfere with the functioning of the private sector.

Pursuant to Article 9 of the Ombudsman Act[38], all proceedings before the Ombudsman are informal and free of charge.

37 The Administrative Court Decision I U 808/2016 of 22 February 2017.

38 Official Gazette RS, No. 69/17 – official consolidated text.

National Assembly of the Republic of Slovenia

Pursuant to Article 61 of the ZVOP-1, the National Assembly of the Republic of Slovenia has a special working body for monitoring the situation in the field of personal data protection.

Question 10

An individual who believes that the controller or someone else is violating the GDPR or the ZVOP-1 in the part still in use may file a complaint with the Information Commissioner for infringement of the right to protection of personal data. The latter initiates an inspection procedure pursuant to the Inspection Act and performs the determination procedure and then takes the appropriate decision. If the Information Commissioner as an inspection body finds the infringement, in accordance with the minor offences provisions of the valid ZVOP-1, it may also impose a sanction on the offender in the form of a fine, which is statutory in the range depending on the gravity of the infringement.

However, if an individual believes that the infringement of his or her rights related to the protection of personal data has occurred and that the infringement has already ceased, he or she may file an action before the Administrative Court to establish that the infringement existed. If an individual suffers damage due to infringement, he or she has the opportunity to file a claim for damage with the ordinary court of general jurisdiction.

Legal action is necessary and preferential, which means that the court, both the regular and the administrative, must complete it as quickly as possible. In the course of action, the public is, in principle, excluded. An individual may also ask the court to impose upon the personal data controller the suspension of any processing of the personal data in the dispute for the time before deciding on the applicant's action.[39]

Question 11

Draft Article 128 of the new ZVOP-2[40] determines the ways of applying the provisions of the GDPR with regard to administrative penalties and fines and deciding on minor offences under this part of the Act. The draft Article is important in terms of designating a supervisory and minor offences authority, transferring (converting) administrative fines

39 Information Commissioner, *Vložitev prijave [Filing an application]*, www.ip-rs.si/protect-private-data/rights-of-individual.

40 Government of the RS, *EVA proposal: 2018-2030-0045, Zakon o varstvu osebnih podatkov, 6 March 2019*, www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/Mandat_2018-2022/Zakonodaja/ZVOP-2_6.3.19_splet.pdf.

into minor offences and deciding on (too) strict administrative fines under the GDPR. Its content provides legal certainty in the area of minor offences as part of criminal law.

Pursuant to draft article 76(1) ZVOP-2, the Information Commissioner must decide on prescribed infringements and administrative fines referred to in article 83 GDPR as minor offences within the competence of the minor offences authority under the provisions of the Minor Offences Act, unless otherwise provided by ZVOP-2. The ZVOP-2, therefore, defines the incriminated infringements (definitions, elements thereof) from the GDPR as minor offences within the meaning of the Minor Offences Act, and their sanctions as sanctions for minor offences (only criminal offences and minor offences exist under Slovenian criminal law). The draft provision also stipulates that article 17 of the Minor Offences Act, a systematic provision of the minor offences law regarding the determination of the range of fines by regulations of the RS, shall not apply.

It is premature to report on the rest of the draft ZVOP-2 concerning sanctions and other consequences of infringements of the GDPR or the ZVOP-2 or other regulations governing this area.

Question 12

Slovenian Obligations Code[41] provides for the possibility of just monetary compensation for non-pecuniary damage (article 179) for breach of personal rights. Slovenian case law has already dealt with the cases of payment of compensation for non-pecuniary damage for suffering mental distress, fear, the defamation of good name or reputation, and truncation of other personality rights due to an unlawful and unauthorised processing of personal data contrary to the purpose for which they were collected.

The Obligations Code provides in the same article:

> "*The amount of compensation for immaterial damage shall depend on the importance of the good affected and the purpose of the compensation, and may not support tendencies that are not compatible with nature and purpose thereof.*"

In the assessment of the amount of compensation for non-pecuniary damage the legal standard of equitable monetary compensation shall be applied. The assessment of whether this legal standard has been properly applied constitutes both an individual examination

41 Official Gazette of the Republic of Slovenia, No. 97/07 – official consolidated text, 64/16 CC dec. and 20/18 – OROZ631.

of the damages awarded for each form of damage and of the total damages awarded as well as a comparative test taking into account known cases in the case law.[42]

Question 13

The draft ZVOP-2, in the article regulating the judicial protection of individual's rights, provides that a data subject may authorise a non-governmental organization in the field of personal data or privacy protection in accordance with article 80(1) GDPR a non-governmental organisation in the public interest to seek judicial protection on its behalf in accordance with this Article. Until the GDPR came into force, the Slovenian legislation (ZVOP-1) did not provide for such an option.

The currently valid ZVOP-1 in article 47 provides only for the possibility for the national supervisory authority to cooperate in its work with institutions, associations and non-governmental organisations in the field of protection of personal data or privacy and other organisations and bodies on all issues that are important for the protection of personal data; however, it cannot delegate powers in the part relating to judicial protection.

Pursuant to article 49 of the applicable ZVOP-1, the state supervisory authority may, in the exercise of its competencies, as follows:

- Issue non-mandatory opinions on the compliance of codes of professional ethics, general business conditions or their proposals with regulations in the field of personal data protection,
- Issue non-mandatory opinions, clarifications and views on issues relating to the protection of personal data and their publication on its website or otherwise,
- Prepare and issue non-mandatory instructions and recommendations regarding the protection of personal data in a particular field,

Invite representatives of associations and other non-governmental organisations in the area of personal data protection, privacy and consumers to cooperate.

Currently, there is no registered non-governmental organisation in Slovenia that would meet the conditions set out in draft ZVOP-2. Similarly, we have not found in practice that any non-governmental organisation with the public interest status or without such status would have the power to provide non-mandatory opinions, instructions or

42 Thus, e.g., compensation for fear of suffering amounts to 4–5 average Slovenian net salaries; the Higher Court in Maribor Judgment Cp 860/2018 of 12 October 2018. In the case of severe mental distress suffered by the plaintiff as a result of unlawful and unauthorised access to information about her illness, she was finally assessed a compensation in the amount of 6 average Slovenian net salaries; Higher Labor and Social Court Judgment, No. VDS0006833 of 17 March 2011.

recommendations, or otherwise have a more prominent influence on the functioning of the Information Commissioner.

Question 14

As regards personal data protection issues, the Information Commissioner cooperates with the Human Rights Ombudsman, also as a member of the Ombudsman's Council. Among the non-governmental organisations, special mention should be made to the Consumers Association of Slovenia, which, among other things, performs numerous activities for raising consumer awareness regarding their rights related to the processing of personal data related to their purchases or shopping habits by merchants.

With regard to personal data breaches (Articles 33 and 34 the GDPR), the cooperation of the Information Commissioner with the newly established Cybersecurity Agency, which will act as the regulator and the inspection body in the field of information security, will be essential[43].

In addition, draft ZVOP-2 stipulates that the Information Commissioner shall cooperate with national authorities, the Committee, other competent authorities of the European Union for the protection of individuals with regard to the processing of personal data, and similar Council of Europe bodies, other international organisations, foreign data protection supervisory authorities, institutions, associations, non-governmental organisations in the field of personal data protection or privacy, and other organisations and bodies on issues relevant to the protection of personal data.

D Data Processing for National Security Purposes

Question 15

Constitutional protection of personal data without exception also applies to bodies and agencies that are carriers of the national security system, which include internal security bodies (e.g. police, judicial police, customs and cybersecurity agency), defence (e.g. army), security and rescue (e.g. firefighting, civil protection) and intelligence and counterintelligence activities[44]. Any restrictions on the rights of the individual related to the processing of information about him or her must also be laid down by law for the bodies of the national security system.

43 Information Security Act, Articles 27 and 31; Official Gazette of the Republic of Slovenia, No. 30/18.

44 Resolution on the National Security Strategy of the Republic of Slovenia; Official Gazette of the Republic of Slovenia, No. 27/10.

Thus, the 2004 ZVOP-1 stipulated that an individual's right to be informed about the processing of his or her data, to know the purposes and content of the data being processed, and to supplement, correct, block, erase and object, may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or taxation reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others. Restrictions could only be set to the extent necessary to achieve the purpose for which the restriction was stipulated.

The approach to limiting the rights of the individual in draft ZVOP-2 was already described in answer to Question 1.

The Constitutional Court of the Republic of Slovenia[45] in the procedure for reviewing the constitutionality of the Information Commissioner in July 2014 repealed all provisions of the Electronic Communications Act[46], which prescribed mandatory preventive and indiscriminate storage of specific traffic data in connection with the use of telecommunications services (telephone services in the fixed and mobile networks, Internet access, e-mail, internet telephony), and by which the Directive 2006/24/EC was transposed into Slovenian law. Under the aforementioned law, operators were obliged to store information on a person's identity, type of communication means and the time, place and frequency of communication for 14 (telephone calls) and 8 months (internet).

The Constitutional Court emphasised that, both in terms of volume of persons and data, it is an extremely invasive interference with the information privacy of the entire population, and so in the absence of objective criteria for such data retention, the measure does not meet the criterion of necessity or the criterion of proportionality in the narrow sense. It also warned of the significant risk that unauthorised persons would be able to access the data, or that the data would be used for illegal purposes and the sense of constant control that such a measure produces on individuals. Unlike Directive 2006/24/EC, the Electronic Communications Act did not restrict the compulsory retention of traffic data to certain (serious) offences. The controversial provisions of the Electronic Communications Act were repealed retroactively, so the Constitutional Court ordered the immediate destruction of all the stored data.

45 The Constitutional Court Decision U-I-65/13-19 of 3 July 2014.

46 Official Gazette of the Republic of Slovenia, No. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – CC dec., 81/15 and 40/17.

From the aforementioned decision of the Constitutional Court onwards, law enforcement agencies have access to traffic, location and other data on the use of telecommunication services only on the basis of a court order issued pursuant to the Criminal Procedure Act[47] if there are grounds for suspecting that it has been committed, executed or prepared or organised a crime for which the perpetrator shall be prosecuted *ex officio* and it is necessary to obtain traffic information on the electronic communications network to detect this crime or perpetrator. Only data on telecommunication services used by a particular individual that the operator is obliged to keep for the prescribed period for billing for services or services may be subject to access or management of telecommunications infrastructure.

47 Official Gazette of the Republic of Slovenia, No. 32/12 – official consolidated text, 47/13, 87/14, 8/16 – CC dec., 64/16 – CC dec., 65/16 – CC dec., 66/17 – ORZKP153,154 and 22/19.

Spain

Antonio Segura Serrano and Julián Valero Torrijos[*]

A Setting the Scene

Question 1

The implementation of the General Data Protection Regulation (hereinafter "GDPR") in Spain has been carried out mainly through Organic Law 3/2018, 5 December, on Personal Data Protection and Guarantee of Digital Rights (hereinafter "LOPDGDD").[1]

With regard to the regulation on administrative procedure, the legal obligation (article 89(1)(c) GDPR) about the verification of those data relevant for administrative decisions has been reinforced and consent is no longer an appropriate basis for this purpose. Consequently, Law 39/2015 on Administrative Procedure has been amended so that any interested person may exercise the right to object, except if sanctioning or inspection powers are affected. Also within the scope of the legal obligations related to article 87 GDPR, when a public body must publish an administrative act as a requirement for its effectiveness, those concerned can only be identified by their name and surname and four random digits of their ID number.

Concerning archiving for public interest purposes (article 89.1 GDPR), the requirement that the necessary technical and organizational measures should be adopted has resulted in the obligation to respect those set out in the National Security Scheme (approved by Royal Decree 4/2010) in order to comply with the level of appropriate security (article 32 GDPR).

Health data regulation has also been updated to the GDPR framework. On the one hand, as a rule, access to medical records for judicial, epidemiological, public health, research or teaching purposes must be carried out separating personal data from those referred to healthcare activity, except if patient's consent is obtained. However, some exceptions are laid down by 17th additional provision LOPDGDD according to article 89 GDPR in order to allow research activities.

---

* Antonio Segura Serrano: Associate Professor of Public International Law at the University of Granada, Spain. Julián Valero Torrijos: Professor of Administrative Law at the University of Murcia, Spain.

1 LOPDGDD www.boe.es/buscar/act.php?id=BOE-A-2018-16673. All webpages referred to were last visited on 27 October 2019.

Several legal provisions have also been passed (articles 87-90 LOPDGDD) to strengthen workers' rights in labour environments according to article 88 GDPR: transparency requirements have been set up, proportionality must be taken into account when surveillance measures are going to be adopted and participation of workers' representatives is required.

However, some other areas are still under an out-of-date regulation from the perspective of the GDPR. Even though the Organic Law of Judicial Power (hereinafter "LOPJ") was also modified in December 2018, that reform only affected to certain competence rules and the use of ICT. However, an explicit reference to the 1999 data protection legislation, adopted under Directive 95/46/EC,[2] is still made by article 236 bis LOPJ. Therefore, although article 23.1.f. GDPR makes it possible to justify the existence of restrictions on certain rights and principles in this field, this authorisation to Member States is subject to basic guarantees that are not compatible with such an updated legal framework.[3]

Article 23.1.d) GDPR allows some restrictions on a data subject's rights if necessary to safeguard the prosecution or enforcement of criminal offences and sanctions according to Directive (EU) 2016/680,[4] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Although LOPDGDD has stated that Organic Law 15/1999, on personal data protection (hereinafter "LOPD") will be in effect until then, the abovementioned Directive is directly applicable since 6 May 2018 and, where appropriate, it will be necessary to interpret its provisions in accordance with EU law since it has not been adopted by Spain yet.[5] Precisely, the EU Commission has decided to refer Spain to the Court of Justice of the European Union (hereinafter "CJEU").[6]

---

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31 (hereinafter "Directive 95/46/EC").

3 J. Valero Torrijos, 'La incidencia en el ámbito judicial del Reglamento General de Protección de Datos Personales desde la perspectiva de la transformación digital', in M.F. Gómez & M. Fernández (Ed.), *Modernización digital e innovación en la Administración de Justicia*, Cizur Menor, Thomson Reuters-Aranzadi, 2019, pp. 110-116.

4 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

5 J. Delgado Martín, *La protección de datos personales en el proceso penal* (El Derecho.com), https://elderecho.com/la-proteccion-datos-personales-proceso-penal-directiva-2016-680.

6 European Commission Press Release 25 July 2019, europa.eu/rapid/press-release_IP-19-4261_en.htm.

Question 2

Spanish law does differentiate between the right to respect for private life and the right to data protection. However, this legal status is the end-result of a process of increasing identification and affirmation of the autonomous right to data protection. Indeed, the Spanish Constitution of 1978 had provided in article 18.4 for the protection of the latter in a negative way. Therefore, originally the right to data protection was linked to the protection of the right to respect private life,[7] which was itself guaranteed in article 18.1 of the Constitution. This link was apparent from Organic Law 1/1982, on the civil protection of the right to honour, to personal and family privacy and to the own image, which provided in its transitional provision no. 1 that violations of the right guaranteed in article 18.4 of the Constitution would find a remedy in said Organic Law until proper and autonomous remedies were established. However, some commentators have always maintained that article 18.4 included a new fundamental right, even if not properly spelled out by the Constitution.[8]

Organic Law 5/1992, on the automated processing of personal data (hereinafter "LORTAD"), was the first one adopted to implement article 18.4 of the Spanish Constitution. This Organic Law was later superseded by LOPD, adopted in order to transpose Directive 95/46/EC. It is stated that both Organic Laws have considered the right to data protection as an autonomous right, although still linked to the right to respect for personal life.[9]

The Spanish Constitutional Court has also adopted a clear inclination to consider the autonomy of the right to data protection. Even if the first rulings used to link it to the right to respect for private life,[10] the landmark judgment adopted in 2000 has confirmed ever since the autonomous character of the right to data protection.[11] Indeed, the right to data protection has a wider reach compared to the right to respect for private life, as the former protects also data which is already public. In addition, data protection is not only a right to freedom, but it gives the citizen a group of positive powers to control personal information as well. Importantly, this conclusion was adopted by the Constitutional Court applying article 10.2 of the Constitution, whereby fundamental rights shall be interpreted

7 A. Troncoso Reigada, *La protección de datos. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010, p. 71.

8 A. E. Pérez Luño, *Derechos humanos, Estado de Derecho y Constitución*, Madrid, Tecnos, 1984, p. 370; P. Lucas Murillo de la Cueva, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990.

9 Troncoso Reigada, 2010, pp. 72-78.

10 Judgment of the Constitutional Court 254/1993, 20 July 1993, ECLI:ES:TC:1993:254; Judgment of the Constitutional Court 143/1994, 9 May 1994, ECLI:ES:TC:1994:143; Judgment of the Constitutional Court 11/1998, 13 January 1998, ECLI:ES:TC:1998:11.

11 Judgment of the Constitutional Court 292/2000, 30 November 2000, ECLI:ES:TC:2000:292; see also Judgment of the Constitutional Court 290/2000, 30 November 2000, ECLI:ES:TC:2000:290.

in accordance to international treaties to which Spain is party. Therefore, the Constitutional Court took into account several international texts, including the Charter of Fundamental Rights of the European Union (hereinafter "Charter") well before its binding force was established by the Treaty of Lisbon.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The Agencia Española de Protección Datos (hereinafter "AEPD"), the Spanish National Supervisory Authority (hereinafter "NSA") has published a report on privacy policies in the online environment related to four areas: hotels, transport, e-commerce and insurance.[12] Although it emphasizes the need to detail all the purposes for which data are processed, the report finds it admissible to sort the aims of data processing by categories in order to make it easier for the user to understand how they will be used. When a legitimate interest is claimed as a legal basis for data processing, the AEPD refuses generic expressions and requires a more detailed explanation.

As the superseded LOPD established an obligation to register files before the AEPD, a certain experience had been acquired by data controllers when it comes to evaluating the purpose of data processing. Regarding the public sector, a legal provision obliges them to publish their Record of Processing Activities as a transparency measure (article 6 bis of Law 19/2013), which should imply that previously they have to evaluate if general principles are respected, the purposes of data processing from the perspective of their own competences and, likewise, the period for which data will be stored.

The AEPD has had the opportunity to set the scope of article 5 GDPR in several official guides.[13] Thus, as regards video-surveillance processing for security purposes, it should be noted that this is possibly one of the most contentious areas as many of the sanctions imposed so far under the GDPR refer to this kind of processing. More recently, the AEPD has published a specific guide on the application of the principle of privacy by design, which emphasizes the importance of data minimization.

Due to the short period elapsed since the GDPR came into force, there have been no judicial decisions on the aspects referred to in the question but the AEPD has had the opportunity to express its interpretation in several reports. Thus, with regard to using data

12 This report is available at www.aepd.es/media/estudios/informe-politicas-de-privacidad-adaptacion-RGPD.pdf.

13 All the AEPD guidelines are available at www.aepd.es/guias/index.html.

for purposes other than those that initially justified its collection and processing, it has been raised the need to cross-check clinical and administrative databases for the identification of risk factors and for the surveillance of pathologies which declaration is not compulsory according to public health rules.[14] Even admitting that consent would not be necessary, a restrictive interpretation has been emphasised by the AEPD since public health legislation itself uses expressions such as 'strictly necessary' or 'essential'. Consequently, general interconnections based on public interest would not respect article 5 GDPR requirements.

Regarding transfers of data between public Administrations,[15] the AEPD requires not only a legal authorisation but an analysis under the criteria of article 6(4) GDPR to be made by the assigning entity as well. Particularly, it has to assess if the reasons that justify data transfers are compatible with those that justified their collection, initially based on a public interest task. However, the AEPD states that, even in the case of incompatibility, in certain circumstances and respecting the legal guarantees (article 23.1 GDPR) data processing would be lawful even without consent of data subjects, unless special categories of data are involved (article 9 GDPR).

Question 4

LOPDGDD includes several provisions based on legitimate interest when enabling certain processing of personal data. Council of State suggested this measure as a solution to enable data controllers an adequate approach to GDPR.[16] Specifically, certain *iuris tantum* presumptions favourable to the prevalence of legitimate interest are legally established if the requirements set out in the regulation are met: this is the case of natural persons' contact details when acting as entrepreneurs or professionals (article 19), credit information systems (article 20) and some commercial operations (article 21). Otherwise, if the legal provisions are not fulfilled, the controller must carry out an evaluation of all the affected interests, but this does not necessarily lead to the unlawfulness of data processing.[17]

Likewise, the Spanish Parliament has promoted a new regulation on certain digital rights in which, although legitimate interest is not explicitly alluded to, it can be understood that processing is fairly based on it if the data controller correctly evaluates all the

14 Report *121/2018*, available at https://www.aepd.es/es/documento/2018-0121.pdf.
15 Report *175/2018*, available at https://www.aepd.es/es/documento/2018-0175.pdf.
16 Report *757/2017*, www.boe.es/buscar/doc.php?id=CE-D-2017-757.
17 J. Fernández-Samaniego & P. Fernández-Longoria, 'El interés legítimo como principio para legitimar el tratamiento de datos', in A. Rallo (Ed.), *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019, pp. 181-185.

implications according to the legal requirements.[18] This would be the case, for example, of labour activities (arts. 87-91 LOPDGDD). Bearing in mind this economic context, a recent judicial decision by a lower court considers unfair using video-surveillance recordings if, as article 89 LOPDGDD requires, workers had not been previously informed about the specific purpose of the data processing. Consequently, the court does not admit that the article 88 GPDR exception would be applicable.[19]

Anyway, it is necessary to highlight that judicial decisions on these issues are still very scarce. However, there is one remarkable exception: LOPDGDDD modified the electoral legislation in order to allow parties to process personal data relating to political opinions 'in the public interest only when adequate guarantees are offered'. This provision (article 58 bis Law 5/1985 on the General Electoral System) had an enormous social impact as it has been declared void by the Constitutional Court.[20] According to the Court's interpretation, it did not identify what that essential public interest really was and, furthermore, it did not state the rules and guarantees that justify such a limitation of the fundamental right to data protection. Moreover, in this case, the Court did not understand legitimate interest as a lawful basis since data controllers are not mere private subjects but, on the contrary, essential instruments for political participation and, consequently, the Court states that they carry out a public task.

As previously explained, the AEPD has emphasized the need to specify those legitimate interests on which data processing is based. It has considered inadequate generic or abstract expressions (i.e. necessary information, get to know you better…), and it has also recommended data controllers to document the evaluation of all the affected interests.[21] Regarding public bodies, unlike other Member States' NSAs, the AEPD considers that legitimate interest is not applicable even when they act beyond the scope of their public tasks (i.e. commercial activities)[22].

Regarding mail preference services for marketing transmissions, the AEPD requires a minimum level of diligence consisting of having previously checked the exclusion lists.[23] As regards the justification of access to data relating to academic marks, it admits economic dependence as a legitimate interest without prejudice to the right of opposition.[24] While in the case of data collection by banks, the AEPD has based on article 6.1.f) GDPR the

18 F.J. Sempere, 'Interés legítimo en el tratamiento de datos: análisis, ponderación y supuestos prácticos', *Privacidad lógica*, 5 March 2019, www.privacidadlogica.es/interes-legitimo-en-el-tratamiento-de-datos-analisis-ponderacion-y-supuestos-practicos.

19 Judgment of the Social Court 3 of Pamplona, 18 February 2019, ECLI: ES:JSO:2019:281.

20 Judgment of the Constitutional Court 76/2019, 22 May 2019, ECLI:ES:TC:2019:76.

21 AEPD report available at www.aepd.es/media/estudios/informe-politicas-de-privacidad-adaptacion-RGPD.pdf.

22 AEPD report available at https://www.aepd.es/es/documento/2018-0175.pdf.

23 AEPD report available at https://www.aepd.es/es/documento/2018-0173.pdf.

24 AEPD report available at https://www.aepd.es/es/documento/2018-0036.pdf.

evaluation of customers' solvency index in order to offer them new services if they are properly informed and the exercise of their right of opposition is allowed independently. Although its interpretation is not so flexible when information has been disclosed by third parties in open social networks and is not obtained from public registers or credit information systems.[25]

As far as consent is concerned,[26] no judicial decisions have been found concerning events occurring after the GDPR entry into force.[27] However, the 17th additional provision of LOPDPGD states that consent is to be understood as given for health and biomedical research purposes not only with respect to a specific research but for other related fields as well. More restrictive is the understanding of AEPD when it comes to commercial communications sent by electronic means: it fined an airline company for not having correctly configured the use of cookies, although the AEPD's decision in this case is not directly based on GDPR provisions but on the information society services and the electronic commerce legal framework.[28]

The most relevant case so far handled by the AEPD in application of the GDPR is undoubtedly the one concerning Professional Football League's app, not only because of the media coverage but also for the € 250,000 sanction imposed. In this case, the AEPD considers that the system for the activation of the microphone and the location of the device does not comply with GDPR consent requirements. Even more, the NSA demands a reinforcement of transparency because data processing is considered to be certainly intrusive.[29] Moreover, it remarked that consent withdrawal demanded an undue effort considering the ease of providing it initially.[30]

Question 5

From a legal point of view, this topic has gained some traction at the national level by way of the use of cookies by content providers. Cookies have been governed in Spain by the

25 AEPD report available at https://www.aepd.es/es/documento/2017-0195.pdf.

26 For an interpretation of article 11 LOPDGDD from the perspective of GDPR requirements, M. Vilasau Solana, 'Las exigencias de información en el RGPD y en la LOPDGDD, ¿contribuyen a la formación de un consentimiento de mayor calidad?, in R. García & B. Tomás (Ed.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado*, Valencia, Tirant lo Blanch, 2019, pp. 218-220.

27 For the analysis of case law prior to GDPR entry into force, A. Puente Escobar, 'Principios y licitud del tratamiento', in A. Rallo (Ed.), *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019, pp. 129-131.

28 Resolution PS/300/19 https://www.aepd.es/es/documento/ps-00300-2019.pdf.

29 In short, when a 'listening' device comes on stage a qualitative approach is needed since other fundamental rights and freedoms may be affected. Regarding this idea, R. Martínez Martínez, 'Internet de los objetos, domótica e inteligencia artificial: la nueva frontera del derecho a la vida privada y familiar', *Diario La Ley*, Nº 31, 2019, p. 2.

30 Resolution PS 326/2018 https://www.aepd.es/es/documento/ps-00326-2018.pdf.

obligations provided for in the second paragraph of article 22 of Law 34/2002, on services of the information society and electronic commerce (LSSI). However, cookies may be exempted if they: 1) only allow communication between the user's equipment and the network, and 2) strictly provide a service expressly requested by the user. In 2013, the AEPD produced a "Guide on the use of Cookies", according to which the legal obligations imposed by the applicable provisions are two, namely: the duty of information and obtaining consent.

However, the extant legal situation has been criticized by some scholars. Indeed, tacit consent by the data subject may still be admissible, even if article 1.2 LSSI provides for the preservation of data protection. Second, if the content to be accessed by the user is made conditional to the previous acceptance of the cookie or, even worse, before opening the main web page of the provider then it is difficult to state that the data treatment has been consented. Likewise, if the treatment is not necessary for the access to the information or the provision of the service then it is hard to label the consent as freely given.[31] Moreover, the provision set up in article 22.2 LSSI is also insufficient because: 1) it only applies to services provided for consideration and thus it does not apply to free services, and 2) it does not cover the abusive processing which results from web browsing.[32] In sum, data processing flowing from the use of cookies or otherwise in exchange for access to free information or content in the web has been allowed until now under Spanish Law.

Prior to the entry into force of the LOPDPGDD, and with regard to the issue of legitimacy for the processing of personal data, the AEPD has produced some specific reports on the interpretation that should be given to the GDPR's provisions on this matter. In this sense, the reports reiterate the AEPD's criteria that the GDPR puts on equal footing the legitimizing grounds set up in its article 6, compared to the provisions of the old Organic Law 15/1999 for which consent became the central axis of the right to data protection. These reports assess what legitimizing grounds other than consent apply to the various kinds of processing, including the one provided for in article 6(1)(b) GDPR.[33]

Question 6

The political situation in Spain is currently unsteady and therefore those legal reforms that should be adopted by the Parliament have not been passed yet. In this sense, in compliance

31 J. Valero Torrijos, "Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado", en J. Valero Torrijos (coor.), *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica*, Cizur Menor, Thomson Reuters, 2013, pp. 58-60.

32 Ibid.

33 AEPD, *Memoria Anual*, 2018, Madrid, pp. 11-12.

with the criteria established by the CJEU,[34] the need has been raised in Congress to promote the reform of the Law 25/2007, 18 October, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

Apart from this issue, article 11 LOPDGDD obliges to inform data owners when their information is collected, so that they can exercise their right of opposition according to article 22 GDPR. Likewise, article 28 LOPDGDD obliges both the data controller and the data processor to adopt the appropriate technical and organizational measures to ensure compliance with GDPR requirements. Particularly, it obliges to take into account the greater risks arising from the use of profiles in some areas. In this respect, the AEPD has made it compulsory to carry out a DPIA for data processing that involves automated decision-making or that largely contributes to take such decisions.

There are also several legal provisions relating to the adoption of automated decisions by public entities. Article 41 Law 40/2015, on the Legal Regime of Public Sector, requires the setting up of a mechanism for auditing the information system and its source code, as well as pointing out the public authority responsible for the decision in the event of contestations. Consequently, administrative appeals settled by a public authority would comply with the provisions of article 22.2.b) GDPR, since it does guarantee human intervention. Specifically in the tax area, article 96.4 Law 58/2003 requires the approval of applications used for the exercise of administrative powers.

Question 7

The Spanish NSA adopted its first Resolutions on the right to erasure ("right to be forgotten") in 2007,[35] according to the increasing demands from Spanish citizens, who have been a kind of pioneers in this field.[36] However, search engines like Google have labelled this kind of protection as censorship. But, on the basis of the principles of consent and legitimate purpose, the AEPD has always decided that search engines were obliged to erase information and deindex links considered obsolete, or personal data whose divulgation does not respond to any legitimate purpose, or if those engines do not use the exclusion protocols, such as "robot.txt", already used by website publishers. In this process, the AEPD

34 Judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, and Kärntner Landesregierung,* ECLI:EU:C:2014:238, in particular para. 55.

35 AEPD, Resolution TD/00266/2007; AEPD, Resolution TD/00463/2007.

36 AEPD, *Memoria Anual*, Madrid, 2013, p. 31.

has been careful to balance the right to be forgotten with the right to freedom of expression and information.[37]

In accordance to the *Google Spain* case adopted by the CJEU,[38] the AEPD and the Audiencia Nacional (with jurisdiction over decisions adopted by the AEPD) have followed suit protecting the data rights of claimants as against Google Spain SL, which appealed those decisions systematically. However, a new issue has opposed the AEPD against Google again. The search engine used to inform website publishers about the content deindexing of searches that affected them when implementing the right to be forgotten. This led the AEPD to impose a 150,000 euro fine to Google in 2016. This fine has later been declared void by the Audiencia Nacional.[39]

On the other hand, the Supreme Court of Spain (Third Court Room, with jurisdiction on administrative law cases) has adopted several decisions admitting many of the Google's appeals.[40] The Supreme Court's judgment is based on the absence of Google Inc.'s legal standing, as it is incorporated in California. This rather unreasoned argument may be confronted with the argument developed by the First Court Room (with jurisdiction on civil law cases),[41] which in turn seems in accordance with the CJEU in the *Google Spain* case. However, the Third Room has continued to decide that the only responsible for the data processing is Google Inc., which in turn may not be the object of a claim in Spain as it is based abroad, a result that does not effectively protect personal data from a material point of view.[42] On the other hand, the Constitutional Court has materially extended the right to be forgotten to include internal search engines used by website publishers,[43] but not the information included in their website pages by publishers,[44] a result very much criticized from some quarters.[45]

37 P. Simón Castellano, *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, Barcelona, Bosch, 2015, pp. 204-221.

38 Judgment of 13 May 2014, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

39 Judgment of the Audiencia Nacional 1801/2019, 23 April 2019, ECLI:ES:AN:2019:1801.

40 See, among many other, Judgment of the Supreme Court 1055/2016, 11 March 2016, ECLI: ES:TS:2016:1055; Judgment of the Supreme Court 964/2016, 14 March 2016, ECLI: ES:TS:2016:964; Judgment of the Supreme Court 3721/2016, 21 July 2016, ECLI: ES:TS:2016:3721.

41 Judgment of the Supreme Court 1280/2016, 5 April 2016, ECLI: ES:TS:2016:1280.

42 P. Lucas Murillo de la Cueva, "El Tribunal Supremo y el derecho a la protección de datos", in R. García Mahamut and B. Tomás Mallén (dirs.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado*, Valencia, Tirant lo Blanch, 2019, p. 204.

43 Judgment of the Constitutional Court 58/2018, 4 July 2018, ECLI:ES:TC:2018:58.

44 J. López Calvo, "Últimas resoluciones judiciales sobre el derecho al olvido. Sobre la inalterabilidad de las hemerotecas digitales", *Diario La Ley Ciberderecho*, nº 20, 2018.

45 P. Romero, "Insólito límite del Constitucional a la libertad de información: ordena capar una búsqueda en una hemeroteca por el 'derecho al olvido'", *Público*, 26 June 2018, www.publico.es/sociedad/derecho-olvido-insolito-limite-constitucional-libertad-informacion-ordena-capar-busqueda-hemeroteca-derecho-olvido.html.

Nevertheless, in 2018 the right to be forgotten has been included in a wider sense by the LOPDGDD, which sets out this right regarding Internet searches (article 93) and social networks or equivalent services (article 94), therefore going beyond the GDPR in consolidating the case-law in this field.[46]

Question 8

The now superseded LOPD was largely adopted in order to transpose Directive 95/46/EC, but did not implement any measure so as to achieve a balance between the right to data protection and freedom of expression as provided for by article 9 of said Directive. Thus, the relationship between both fundamental rights has been solved by the Constitutional Court's case-law from the 1980s,[47] which has declared the superiority of freedom of expression, wherever the information was of public interest and truthful.[48] This case-law has been followed by the AEPD ever since.[49]

However, the recent LOPDGDD has been used by the legislator to offer a slightly different balance between both fundamental rights protected by the Spanish Constitution. Indeed, article 85 GDPR has been adapted to national law through two provisions included within Title X devoted to the "Guarantee of digital rights". This Title X goes well beyond what is required by GDPR and sets out digital rights such as the right to Net neutrality, the right to universal access to the Internet, the right to digital security, and the right to digital education, among other rights. The two mentioned provisions are article 85 and article 86 LOPDGDD.

First, article 85.1 LOPDGDD states: "Everyone has the right to freedom of expression on the Internet". According to the Constitutional Court case-law on the right to rectification regulated by Organic Law 2/1984,[50] article 85.2, first paragraph LOPDGDD may be interpreted as the defence mechanism that an individual has to protect her honour *vis a vis* informational initiatives or mistakes that may endanger the moral integrity or reputation of the interested person. Moreover, the right to rectification may serve as a complement to the guarantee of a free public opinion, to the extent that a different interpretation of the information published will help the collective interest in reaching the truth, as provided for by the second paragraph of article 85.2 LOPDGDD.

46 A. Rallo Lombarte, "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", in R. García Mahamut and B. Tomás Mallén (dirs.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado*, Valencia, Tirant lo Blanch, 2019, p. 147.

47 See recently Judgment of the Constitutional Court 58/2018, of 4 June, ECLI:ES:TC:2018:58.

48 J. Muñoz-Machado Cañas, "Tratamiento de datos y libertad de expresión e información", in J. Piñar Mañas (dir.), *Reglamento General de Protección de Datos*, Madrid, Reus, 2017, pp. 595-596.

49 AEPD, Resolution nº 27/2005, 24 January 2006.

50 Judgment of the Constitutional Court 168/1986, 22 December 1986, ECLI:ES:TC:1986:168.

Second, article 86 LOPDGDD serves as a complement to the right to rectification, through the setting up of the right to update information in digital media.[51]

This new legal situation will have a huge impact on digital media and social networks, and has been criticised by some experts in the field. It is said that the new provisions will modify the extant balance, as the right to rectification may be invoked not only as against untruthful information, but also as against information affecting the right to privacy and honour.[52] Furthermore, social media will have to rectify not only information published by the media, but also that published by their users. This may lead them to contract out pre-moderation services, thereby affecting freedom of expression,[53] allowing for censorship through the back-door and with no judicial control.[54]

To this date, there is no Court or NSA decision regarding these new provisions introduced by the LOPDPDD. However, the extant Constitutional Court's case-law in the field of Organic Law 2/1984 will plausibly be applicable.

C Domestic Enforcement of Data Protection Law

Question 9

The Spanish NSA, the AEPD, was set up in 1992 as an independent public body.[55] Similar authorities have also been created by some Autonomous Communities: Catalonia,[56] Basque Country,[57] and, recently, Andalusia.[58] However, their competence extends only to data processing carried out at the regional and local pubic sector level.

---

51 "Every person has the right to request from the digital media the inclusion of a sufficiently visible update notice along with the news that concerns her when the information contained in the original news does not reflect her current situation as a result of circumstances that had taken place after publication, causing damage. In particular, the inclusion of such notice shall proceed when the original information refers to police or judicial proceedings that have been affected for the benefit of the interested party as a result of subsequent judicial decisions. In this case, the notice will refer to the subsequent decision".

52 "Victoria para la libertad de expresión: la nueva Ley de Protección de Datos renuncia a controlar contenidos digitales y a acabar con el anonimato en Internet", *Plataforma en defensa de la libertad de información*, 10 October 2018, http://libertadinformacion.cc/victoria-para-la-libertad-de-expresion-la-nueva-ley-de-proteccion-de-datos-renuncia-a-controlar-contenidos-digitales-y-a-acabar-con-el-anonimato-en-internet/.

53 "La nueva ley de Protección de Datos impacta en los medios de comunicación", *Ayuda ley protección datos*, 23 November 2018, https://ayudaleyprotecciondatos.es/2018/11/23/nueva-ley-proteccion-datos-rectificacion/.

54 T. Castillo, "La nueva ley de protección de datos es preocupante para la libertad de expresión en España: abre la puerta a la censura", *Xataka*, 9 October 2018, www.xataka.com/legislacion-y-derechos/acuerdo-para-ampliar-derecho-rectificacion-a-internet-preocupa-supone-mayor-control-internet-espana.

55 www.aepd.es/.

56 https://apdcat.gencat.cat/en/inici/index.html.

57 www.avpd.euskadi.eus/s04-5213/es.

58 www.ctpdandalucia.es/es.

Specifically, in the case of the AEPD, its President must be elected among persons of recognised professional competence. The selection process call has to be published in the Official Journal (Boletín Oficial del Estado) and the Government will present a proposal to the Parliament after evaluating the candidates bearing in mind their merit, capacity, competence and suitability, which must be ratified by a qualified majority. The term of office is five years and the person elected may only be dismissed for serious breach of duties, incapacity, incompatibility or criminal punishment. A Council with only consultative functions made up of 17 members will advise the President: there will be representatives of the Parliament and of the regional data protection authorities, as well as a broad social, professional and academic representation.

The Spanish NSA has the power to carry out preventive audit plans and to approve Circulars setting out its own interpretative criteria when applying the GDPR and the LOPDGDD. It may also fine data controllers/processors and, if necessary, adopt preventative measures. Apart from fines, sanction consists of a warning in minor cases and when a public body commits the infringement. However, in the case of complaints introduced by data subjects article 37 LOPDGDD provides for a procedure before the controller/processor's Data Protection Officer (hereinafter "DPO") under the AEPD supervision.

With regard to its 'enforcement record' under the GDPR, 139 procedures have been finished according to the AEPD's official website. Some important sanctions should be highlighted: the above-mentioned 250,000 euro fine imposed to the Professional Football League; an airline company was punished with 18,000 euro; a telephone company has been penalized with two sanctions that came to more than 40,000 euro; and several video surveillance infringements have been punished with fines between 4,800 and 20,000 euro.

Question 10

Article 50 LOPDGDD establishes the obligation to publish AEPD decisions related to enforcement powers.[59] This provision reinforces certainty since it allows to know the AEPD interpretative criteria. In addition, an official report is published every year.

Beyond the exercise of sanctioning powers, the AEPD is making a significant institutional communication effort within the framework of its Corporate Social Responsibility Plan.[60] AEPD's commitment to data controllers and professionals must be

59 Its decisions are available through a useful search engine on its website https://www.aepd.es/es/informes-y-resoluciones/resoluciones.

60 AEPD's social commitment has been included in *Marco de Actuación de Responsabilidad Social de la AEPD (2019-2024)*. This document is available at www.aepd.es/media/plan-rs/marco-responsabilidad-social-AEPD.pdf.

emphasized, although it would be advisable to reinforce participation as a "good governance" tool.

With regard to the promotion of preventive measures, several initiatives have been launched, among which the following stand out:

- Availability of free tools to facilitate compliance with the GDPR and the LOPDGDD, especially for low risk data processing and formal obligations;
- Publication of the Agency's legal team reports in response to queries of greater interest made by data controllers;
- Publication of specific guides on relevant areas (education, Internet privacy and security, local Administration) and recommendations to facilitate compliance with some essential obligations such as privacy by design, DPIA, management and notification of security breaches or risk evaluation;
- Publication of practical guides and studies for some types of data processing: use of fingerprints, drones, apps for mobile devices, video-surveillance or publication of administrative acts;
- Implementation of a priority channel for communicating the dissemination of sensitive content on the Internet and requesting its removal.[61]

Question 11

As the LOPDGDD came into force in December 2018 and the latest AEPD published report corresponds to the year 2018,[62] there is no official and updated information on the sanctions imposed under GDPR provisions. However, there is a general tendency to apply the warning sanction and, where appropriate, a requirement to adopt corrective measures in cases of minor infringements.[63]

With regard to the role of DPOs in order to solve complaints from data subjects, 863 have been satisfactorily addressed during 2018 and 2,079 up to 15 May 2019[64]. Therefore, it seems to be an effective way to ensure effective respect for the rights of data subjects.

Warning is the only punishment for public bodies' infringements, although the Ombudsman must be notified of the sanctions imposed to them and disciplinary proceedings against public officials may be recommended by the AEPD. The publication

61 This recent tool is available at www.aepd.es/media/infografias/infografia-canal-prioritario.pdf.

62 This official report is available at www.aepd.es/media/memorias/memoria-AEPD-2018.pdf.

63 J. Sempere Samaniego, 'Primeras resoluciones sancionadoras de la Agencia Española de Protección de Datos con el RGPD', *Privacidad Lógica*, 29 April 2019, www.privacidadlogica.es/primeras-resoluciones-sancionadoras-de-la-agencia-espanola-de-proteccion-de-datos-con-el-rgpd/.

64 AEPD Press Release 21 May 2019, available at https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/dos-de-cada-tres-reclamaciones-que-se-envian-al-dpd-se.

of sanctions in the official journal is also stated by article 77 LOPDGDD, but only for the most serious cases.

Question 12

According to article 23 of Directive 96/45/EC, the now superseded LOPD provided in its article 19 for a right to compensation for the data subjects in case of a breach of the provisions of this LOPD. It also stated that the applicable liability regime would be that of Administrative law (according to Law 40/2015), in case of public filing systems, while in case of private filing systems that liability would be ascertained by Civil law Courts (according to article 1106 Civil Code). However, the liability system set up in Organic Law 1/1982 on the civil protection of the right to honour, personal and familiar privacy and the own image has also been applied by Courts in Spain because of the close link between these constitutional rights and the data protection right, also protected by the Spanish Constitution in the very same article 18.[65]

Now, Organic Law 3/2018 (LOPDPGDD) has superseded the LOPD of 1999. However, no provision has been included in the LOPDGDD on compensation for damages, which in turn makes the GDPR the only regulation applicable in this field in Spain, according to its directly applicable character. Nevertheless, the three systems of liability just mentioned will continue to be applied by Courts in Spain as the only ways to give legal traction to article 82 GDPR.[66]

According to what now is provided for in article 82 GDPR, the Spanish liability system applicable to the field of data protection has always included non-material damages. The definition of non-material damages is no easy task,[67] but the real hurdle rests on its proof. Even if some Spanish case-law has adopted the doctrine derived from Organic Law 1/1982, where damage is presumed and awarded wherever there is a breach (*iuris et de iure*), the liability system provided in now superseded article 19 LOPD was different (*iuris tantum*), so the data subject had to prove the damage. As it is well known, the GDPR does not offer any guide regarding proof, so this issue remains debatable.[68]

65 E. Nieto Garrido, "Derecho a indemnización y responsabilidad", in J. Piñar Mañas (dir.), *Reglamento General de Protección de Datos*, Madrid, Reus, 2017, p. 567.

66 However, the subjective liability system provided for in article 82 GDPR will be substituted for an objective system in Spain wherever the GDPR breach is provoked by a public filing system, *ibid.*, p. 561.

67 J. Puyol Montero, "Derecho a indemnización", in A. Troncoso Reigada (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas, 2010, p. 1277, stating that the Supreme Court has defined it as "inferred pain, suffering, sadness, unease or restlessness that affects the person suffering from it".

68 A. Rubí Puig, "Daños por infracciones del derecho a la protección de datos personales", *Revista de Derecho Civil*, vol. V, nº 4, 2018, p. 82.

Compensation for non-material damages has been very common in the Spanish case-law as a result of the application of article 19 LOPD. Civil law cases where non-material damage has been compensated include breaches such as undue inclusion in databases of consumer credit reporting agencies like Equifax, breaches of the right to be forgotten, illegitimate access to medical records, etc.[69] However, in order to be compensated in Administrative Courts, material and non-material damages are subjected to several conditions: they need to be effective, real and true; economically evaluable; be able to be attributed to a single individual or group of individuals; and the data subject must not be obliged to endure the breach.[70] Additionally, not every non-material damage must result in monetary compensation, as often the case-law has determined that other remedies are available, i.e., the judicial decision itself declaring the breach is sometimes considered a just compensation.[71]

Question 13

Organic Law 3/2018 (LOPDGDD) recently adopted to adapt and complement the GDPR has not implemented any legislative measure in order to facilitate the representative actions provided for in article 80 GDPR. Therefore, representative actions may only be initiated according to the general mechanisms provided for in Spanish law. Collective actions in Spanish law are mainly regulated in the Civil Prosecution Law (Ley de Enjuiciamiento Civil- LEC). Particular attention should be paid to article 11 LEC which provides for the legal standing of consumer and user associations for the exercise of class actions.

Thus, consumer and user associations in Spain have carried out an important activity regarding the legal enforcement of data protection rights, not only for their associates, but for all consumers in general. Recently, as a result of the Cambridge Analytica revelations, one of the largest association, the Organización de Consumidores y Usuarios (hereinafter "OCU") initiated a class action lawsuit against Facebook. The OCU considered that Facebook had breached data protection rights of users as it did not inform or request express authorization from users for the use of their data. The lawsuit defended the interests not only of those directly affected by the alleged data leakage, but of all Facebook users in Spain, some 26 million users and, accordingly, the OCU asked for at least € 200 of compensation for each of them.[72]

69 Ibid., p. 75.

70 U. Aberasturi Gorriño, "El derecho a la indemnización en el artículo 19 de la Ley Orgánica de Protección de Datos", *Revista Aragonesa de Administración Pública*, nº 41-42, 2013, p. 180.

71 Ibid., pp. 200-201.

72 OCU, "Mis datos son míos, Facebook", 30 May 2018, www.ocu.org/consumo-familia/derechos-consumidor/noticias/demanda-colectiva-facebook.

Moreover, another user association called FACUA has lodged five complaints with the NSA (AEPD) against Facebook. In the latest complaint the FACUA argues that Facebook has shared unauthorized sensitive data of its users with third parties (Netflix, Spotify, Bing, and Microsoft).[73] The other complaints related to Cambridge Analytica, the filtering of personal data of users who used a survey app, the hacking of information due to a vulnerability detected in the tokens of the social network, and the breach of the LOPD regarding the procedure used for users to exercise their rights.[74]

Question 14

The AEPD has carried out several activities addressed not only to professional groups, data controllers and processors but also for data subjects and society, an initiative linked to the 2015-2019 Strategic Plan.[75] One of its main axes is to enhance prevention in order to achieve a more effective protection of citizens' rights. Therefore, communication channels have been strengthened, various information campaigns have been promoted and, among other measures, collaboration with media has increased. In this regard, special attention has been paid to minors and education, with the launch of a specialized website.[76]

Within the dissemination activities, the annual Open Day involves not only its own staff but social and professional representatives as well. This workshop is also available on the Internet, which ensures wider dissemination.[77] Likewise, also on an annual basis, the AEPD organises a summer course jointly with the Menéndez Pelayo International University-UIMP.[78]

As regards relations with other public institutions, there is a legal obligation to communicate to the Ombudsman the actions taken by the AEPD in relation to public bodies. In the area of transparency, a joint action with the Transparency and Good Governance Council is also legally stated in order to approve criteria for the evaluation of conflicts between privacy and access to public sector information. A representative of that entity has to be elected as a member of the AEPD Advisory Council.

73 Europa Press, "Facua denuncia ante la AEPD a Facebook por compartir datos sensibles de sus usuarios con terceros", 20 December 2018, www.europapress.es/sociedad/noticia-facua-denuncia-aepd-facebook-compartir-datos-sensibles-usuarios-terceros-20181220165113.html.

74 La Vanguardia, "FACUA denuncia a Facebook ante AEPD por compartir datos de usuarios a tercero", 20 December 2018, www.lavanguardia.com/vida/20181220/453657044742/facua-denuncia-ante-la-aepd-a-facebook-por-compartir-datos-sensibles-de-sus-usuarios-con-terceros.html.

75 This Plan is available at https://www.aepd.es/es/la-agencia/plan-estrategico-aepd-2015-2019.

76 All the information is accessible at http://tudecideseninternet.es/aepd/.

77 The 2019 edition can be seen at https://www.aepd.es/es/la-agencia/transparencia/otro-tipo-de-informacion/sesion-anual-abierta-aepd/11-edicion.

78 The programme of the latest edition is available at www.uimp.es/agenda-linkb.html?id_actividad=64C2&anyaca=2019-20.

A collaboration agreement has been signed between the AEPD and the General Council of the Judiciary (CGPJ) according to article 55(3) GDPR.[79] Formal collaboration has also been promoted with the National Commission on Markets and Competition (CNMC).[80]

D Data Processing for National Security Purposes

Question 15

National security has been fairly recently defined in Spanish law through article 3 Law 36/2015 on National Security. Regarding public security, article 104.1 of the Spanish Constitution governs the activities of law enforcement agencies and includes the concept of citizen security, while its article 149.1.29ª was devoted to public security. However, these two concepts have been interpreted as synonyms by the case-law and literature alike. Recently, Organic Law 4/2015 on the protection of citizen security has been adopted and there are other laws applicable in this field.[81]

After the *Tele2/Watson* case,[82] case-law in Spain has accepted the application of the Charter to data retention for public security purposes. However, national legislation providing for data retention, in accordance to Directive 2006/24/EC,[83] has not been declared invalid as a result of *Tele2/Watson*. Specifically, the Supreme Court of Spain adopted two judgments right after the *Digital Rights Ireland* case.[84] In those two decisions, and after explicitly mentioning article 8 of the Charter, the Supreme Court stated that Law 25/2007 on data retention (LCDCE), implementing Directive 2006/24/EC, was not affected by the *Digital Rights Ireland* case as the LCDCE was already being interpreted in a very restrictive way by national courts.[85] Moreover, after *Tele2/Watson*, the Supreme Court has maintained the same position regarding Law 25/2007. Accordingly, two decisions adopted in 2017, in

79 The full version of this document is available at www.boe.es/boe/dias/2017/11/15/pdfs/BOE-A-2017-13162.pdf.

80 A General Protocol of Activities has been approved, which is available at https://www.aepd.es/sites/default/files/2020-02/protocolo-aepd-cnmc.pdf.

81 O. Tejerina Rodríguez, *Seguridad del Estado y privacidad*, Madrid, Reus, 2014, p. 127.

82 Judgment of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, ECLI:EU:C:2016:970.

83 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

84 Judgment of 8 April 2014 in Joined cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

85 Judgment of the Supreme Court 470/2015, 7 July 2015, ECLI: ES:TS:2015:3436; and Judgment of the Supreme Court 768/2015, 23 November 2015, ECLI: ES:TS:2015:5140.

which the 2016 ECJ's case is taken into account, stated that Law 25/2007 is still perfectly applicable. The rationale of the Supreme Court is based on the guarantees provided by the restrictive interpretation of Law 25/2007, as applied by national Courts until now. Under this restrictive interpretation, data retention is only ordered by a judicial authority and for serious crimes, which in turn will preserve the proportionality principle as mandated by the ECJ.[86] However, this Supreme Court's interpretation has been the object of criticism by the literature, which considers that it does not apply the proportionality principle in the same way it is requested by the ECJ's case-law.[87]

86 Judgment of the Supreme Court 272/2017, 18 April 2017, ECLI: ES:TS:2017:1594; and Judgment of the Supreme Court 400/2017, 1 June 2017, ECLI: ES:TS:2017:2800.

87 J. L. Rodríguez Lainz, "La jurisprudencia del tribunal de Luxemburgo sobre regímenes de conservación preventiva de datos en la Doctrina del Tribunal Supremo", *Diario LA LEY*, nº 9087, 2017, p. 7.

Sweden

Pernilla Norman[*]

Introduction

Sweden introduced the world's first Data Protection Act in 1973.[1] The same year, the first National Supervisory Authority (hereinafter "NSA") in the world, the 'Datainspektionen', was set up. The task of the *Datainspektionen* was to safeguard the application of the Data Protection Act. With the longest history of Data Protection legislation and enforcement in the world, Sweden has extensive case law in the area.

A year after application of the General Data Protection Regulation (hereinafter "GDPR")[2] commenced, the *Datainspektionen* conducted a number of surveys on application and attitudes following the introduction of the GDPR. The result of these were analysed in a report, the Nationell integritetsrapport 2019.[3] Sweden has far reaching goals when it comes to using digitalization both in private and public activities. The handling of personal data, and not the least the general trust and perception of how personal data is processed, is a key factor to success and development in digitalization. The Swedish view on GDPR should thus be put in that perspective.

A Setting the Scene

Question 1

As Sweden has always been in the front as regards data protection and adopted its first legislation already back in 1973, the Data Protection Act (*Datalagen*)[4], a short historical overview can be of interest. The Data Protection Act prescribed that permits be obtained

* Advokat, Partner at Advokatfirman LexIT and PhD candidate at the Faculty of Law, University of Stockholm, Sweden.

1 Datalag (1973:289).

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

3 Nationell integritetsrapport 2019, Datainspektionens rapport 2019:2.

4 Datalagen (1973:289).

from the Swedish NSA, the *Datainspektionen*, to establish a 'computerized' (automized) personal register.

Data protection principles were introduced by the Council of Europe's 'Data Protection Convention' of 1981 (Convention for the protection of individuals with regard to Automatic Processing of Personal Data, also known as 'Convention 108'). A major difference between the Data Protection Convention and the *Datalagen* was that the Convention did not only apply to 'computerized' personal registers, but to all procession of personal data.

EU Directive 95/46/EU of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive) was implemented into Swedish law by the *Personuppgiftslagenin 1998*.[5]

In parallel to the *Datalagen*, separate legal instruments (so called "*registerförfattningar*") were continuously introduced for specific "computerized" personal registers, such as *Patientjournallagen*[6] for "computerized" patient records (later replaced by *Patientdatalagen*[7] regulating the processing of patient data in a wider perspective).

In connection with the entry into force of the GDPR, Sweden adopted a Data Protection Act (*Dataskyddslagen*)[8] where the legislation complementary to the GDPR is collected. A regulation on complementary issues (*Kompletteringsförordningen*)[9] was issued and entered into force at the same time, 25 May 2018. In addition, the system with "*registerförfattningar*" (see above) has been kept. A number of these statutes have been adjusted to comply with the GDPR.

As mentioned above, the national Swedish NSA is the *Datainspektionen*.[10] The *Datainspektionen* is also Sweden's national supervisory authority regarding processing of personal data under the Schengen Convention, that is to say the convention on the EU's customs information systems,[11] the Regulation on the establishment of the EU agency for

5 Personuppgiftslagen (1998:204).
6 Patientjournallagen (1985:562).
7 Patientdatalagen (2008:355).
8 Dataskyddslagen (2018:218).
9 Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.
10 See 3 § Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning, and 2 a § Förordning (2007:975) med instruktion för Datainspektionen (Ordinance on Instructions for the Swedish Data Protection Authority).
11 Convention 27 November 1995.

law enforcement cooperation (Europol)[12], the VIS Regulation,[13] and the Eurodac Regulation.[14]

The Swedish Data Protection Authority's tasks as a surveillance authority are stated in its instructions.[15] It should be noted that the *Datainspektionen* is also to monitor and describe developments in IT regarding issues concerning privacy and technology.[16] Thus, the *Datainspektionen*'s surveillance competence includes the GDPR, as well as the national legal instruments in relation to the GDPR. As concerns these legal instruments, it should be born in mind that it follows from the long history of data protection legislation in Sweden that there is substantial case-law, which to a considerable extent is applicable also to the present situation, i.e. after the entry into force of the GDPR.

There are two areas where the situation in Sweden differs considerably from most other Member States, where Sweden holds a strong and long legal tradition. These are transparency and the use of identification numbers (social security numbers). Thus, these areas are of particular interest when it comes to data protection.

Firstly, Sweden has a longstanding national principle on public access to official documents which is protected in the constitution.[17] The principle is further specified in the Public Access to Information and Secrecy Act.[18] It follows from article 86 GDPR[19] that personal data included in official documents can be made public in accordance with the laws of the Member State concerned. Furthermore, the Council of Europe has already in 1991 adopted a recommendation of access to personal data in public documents.[20] Hence, the GDPR does not prevent the possibility to give public access to official documents

12 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53.

13 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2008] OJ L218/60.

14 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2013] OJ L180/1.

15 Ordinance (2007:975) on Instructions for the Swedish Data Protection Authority.

16 For further description see Datainspektionen's webpage www.datainspektionen.se, also available in English. All webpages referred to were visited 1 February 2020.

17 The so called "offentlighetsprincipen", stipulated in 2 Chapter of Tryckfrihetsförordningen (1949:105).

18 Offentlighets- och sekretesslagen (2009:400).

19 See also recital (whereas) 154.

20 The Council of Europe, Recommendation No. R(91) 10 on the communication to third parties of personal data held by public bodies.

containing personal data. In addition to the stipulation in GDPR, the national Swedish Data Protection Act contains a provision expressly excluding GDPR from being used in a manner that would restrict or prevent the principle on public access to official documents.[21]

Secondly, the other area of special interest is the handling of personal identification numbers (social security numbers), which is widely spread in Sweden. The GDPR opens up for national legislation within this area.[22] The Data Protection Act (*Dataskyddslagen*) contains a stipulation permitting personal identification numbers to be processed without consent only in case it is clearly motivated by the reasons of the processing, the importance of secure identification or other considerable reasons.[23] Thus the main principle is that consent is needed for the processing of personal identification numbers. It should be remembered that the general requirement for legal basis in article 6 and the principles in article 5 of the GDPR must be upheld. The stipulation follows previous regulations and consequently there is considerable case-law in the area. This case law can be summarized with the conclusion that it is somewhat more restrictive from a legal perspective, than the actual situation where personal identification numbers are widely processed in the day to day life of Swedes.

Question 2

Human rights, both the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union is of fundamental importance to data protection in Sweden. It can be said that it is *Datainspektionen*'s main task to "work to ensure that people's fundamental rights and freedoms are protected in connection with processing of personal data, to facilitate the free movement of such data within the European Union and to work to ensure that good practice is observed in credit rating and debt recovery activities."[24]

21 Chapter 1 Section 7 Dataskyddslagen.
22 Art. 87 GDPR.
23 Chapter 3, Section 10 Dataskyddslagen.
24 1 § Förordning (2007:975) med instruktion för Datainspektionen (Ordinance on Instructions for the Swedish Data Protection Authority).

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

In general, it can be said that awareness of the GDPR is fairly high in Sweden. According to the National integrity report 2019, carried out by the *Datainspektionen*, the majority of companies and organisations state that the implementation of GDPR into the businesses has worked well.[25] Nine out of ten citizens are aware of the fact that when browsing the internet information is collected which is sold for marketing purposes. Only three out of ten however, feel they have knowledge of how their personal information is used. In organizations where a Data Protection Officer (hereinafter "DPO") was appointed, the survey found that three out of four DPO's stated that relevant guidelines had been put into place within the organization. Further, organizations without a DPO also expressed awareness of the GDPR. Over all, seven out of ten companies state they have guidelines and have taking actions implementing the GDPR.

As regards the interpretation and practical use of the GDPR-principles (in article 5) the survey shows that a majority of organisations have put processes and routines in place that ensures the upholding of the principles. At the time this report being written (early 2020) there are only two decision by the *Datainspektionen*.[26] However, these decisions have been appealed against, but not yet decided by any court. The first decision by the *Datainspektionen* concerns facial recognition. The situation in that individual case was a bit particular which meant that the decision by the *Datainspektionen* did not relate to the general principles, such as purpose limitation or data minimization. Thus, the principles of purpose limitation and data minimization have not yet been subject of a decision or court proceedings However, as regards the concept of 'fair' processing, there was already prior legislation, the *Personuppgiftslagen*.[27] Hence, there is case-law dealing with this concept.

Also the concept of purpose limitation is well known in Swedish data protection legislation. The requirement of the purpose to be sufficient *specific* has been explained in the preparatory works to previous statutes.[28] In general can be said that the purpose is sufficiently specific if the purpose cannot be realized if the personal data is not processed.[29]

---

25 Nationell integritetsrapport 2019, Datainspektionens rapport 2019:2.
26 Datainspektionen beslut DI-2019-2221, 20 August 2019 and beslut DI-2018-22737, 13 December 2019.
27 Personuppgiftslagen (1998:204).
28 SOU 1999:109 p. 156 and SOU 1998:80 p. 221 f.
29 Öman, Sören, Dataskyddsförordningen (GDPR) m.m. En kommentar, Ed 1:1, Norstedts Juridik 2019, p. 116.

The fact that the purpose must be *legitimate* has caught some interest in the preparatory works. It is considered to have a direct link to the legal grounds set out in article 6.[30] The following list are examples of decisions by the *Datainspektionen* under the previous act, the *Personuppgiftslagen*.

- Personal data cannot be used in the measurement of performance at the workplace.
- The Data protection authority also found that an organisation was not allowed to hand over gathered information about its members to a third party for marketing purposes.
- It was also concluded that a school could not use collected social security numbers of its students to be used to publish the schedules of the students online.
- Lastly, it was found to not be allowed to gather personal information regarding the performance of legislative workers. Although the restriction only becomes relevant if the information is collected by the means of how work is performed and when the workers would take breaks, as well as if the purpose of collection would be in order to find grounds for performance salaries.[31]

According to article 5(c) GDPR, which regulates data minimization, the personal information that is processed should be adequate and relevant in regard to the purpose of collection. In addition, the information gathered cannot be too broad compared to the underlying reason the information was gathered. This is in order to minimize the amount of personal data collected and stored to further protect the individual integrity of people.[32]

As with purpose limitations, there still has not been any Swedish court case that concerns data minimization under the GDPR. However, also here, reference can be made to the situation under prior legislation, the *Personuppgiftslagen*. One example is how the data processing at a company may not be considered relevant or adequate. This became evident in a case concerning a supermarket, which in a few seconds registered personal details of customers buying beer with a degree of alcohol, in order to prevent someone underage from buying the products as sales to persons under the age of 18 was not permitted. The Data Protection Authority came to the conclusion that the purpose to prevent the sales of alcoholic beer to persons under the age of 18 did not require collection of all this personal data from all customers. Thus, it was not an adequate method and therefore was contrary to the *Personuppgiftslagen*.[33]

Another example of a breach of the principle of data minimization concerns the collection of personal information at a company. A company gathered information containing for example the gender, sexual orientation and ethnicity of its employees. The

30 Prop. 2017/18:105 p 47. See also SOU 2001:32 p 122 f where it is noted that the term legitimate does not have an independent meaning in relation to the requirement of the purpose being specified and explicit.

31 Öman, 2019, p. 121.

32 *Ibid*, p 126.

33 Datainspektionen beslut 1978-2004.

reason was to prevent discrimination at the workplace, specifically as regards promotions, salaries, etc. The collection of data was entirely voluntary, without any consequences if not answered. The *Datainspektionen* found that this method violated the *Personuppgiftslagen*. The decision was appealed to the Administrative County Court of Stockholm (*Förvaltningsrätten*), which came to the same conclusion as the *Datainspektionen*, on the following grounds. According to the court, the gathered information would not be a large enough basis for the purpose of the process, which consequently created an unnecessary storage of highly personal information. Furthermore, the court considered the information to be too wide compared to the purpose of its use. Lastly, it concluded that there would be a need for long term storage of the personal information, which would clash with the principal of storage minimization.[34]

From the decisions described above, several conclusions can be drawn. The main conclusion is that the Swedish view concerning the former legislation (*Personuppgiftslagen*) which has to a large extent been transferred into the GDPR, is that when sensitive data, such as social security numbers and facts about ethnicity and sexual orientation etc, are collected, there need to exist a very clear purpose and specific management of said information. Therefore, one could conclude that the Swedish interpretation of the previous legislation and thus the GDPR clearly and accurately follows the wording in the legislation.

Question 4

Regarding consent, one of the legal bases stipulated in the GDPR, article 6(a) provides that personal information can be registered if consent is given to use the information for one or several specific purposes. The term consent is defined in article 4(11) GDPR. There is a burden of proof in that the controller has to be able to show that consent has been given for each specific processing.[35] This is particularly important as a consent can be withdrawn at any time. Furthermore, the principles in article 5(1) GDPR, have to be upheld regardless the legal bases for the processing and thus also when consent is used.

Concerning the legal base legitimate interest, this is stipulated in article 6(f) GDPR. There are no general rules on what constitutes legitimate interest, but what may be considered as legitimate interests needs to be established on a case by case basis. As of yet, there has not been any Swedish court cases dealing with legitimate interests under GDPR. However, the concept applied also under the previous legislation. The following examples illustrates considerations in relation to legitimate interest.

34 The Stockholm Administrative County Court, case 13371-17, judgement 25 June 2018.
35 Art. 7(1) GDPR.

- The Data protection authority found that 'local authorities' (*kommunalförbund*) did not have legitimate interest in a case where the garbage collector kept detailed information of the content of garbage of individual people.[36]
- The Sundsvall Administrative Court of Appeal concluded that a person who requested thousands of grades to perform a study on the correlation between secondary school and high school grades, in fact had a legitimate interest.[37]
- The Stockholm Administrative Court of Appeal in Stockholm concluded that collecting statistics on how the healthcare system works did not serve as legitimate interest.[38]
- The Gothenburg Administrative Court of Appeal held that examining the terms of contract between a parking company and its customers in order to provide feedback was not a legitimate interest.[39]

These examples gives a first impression on how Swedish courts reason in cases relating to legitimate interest. It can be concluded that a clear overstepping of personal integrity, as with the example of the garbage disposal company, cannot be justified on the grounds of legitimate interest. Swedish courts and the *Datainspektionen* seem to be more willing to accept that there is a legitimate interest when the personal data are less intrusive. In addition, research purposes may generally constitute a legitimate interest.

Question 5

The fast development of technology and digitalization means that digital solutions are used in people's everyday life to a large extent. Sweden could be considered as an advanced high-tech country where digital solutions are a widely used in more and more areas. Swedish public authorities have come far in the development of digital public services. Another interesting area is that of payments, as physical money (cash) is being phased out and is no longer accepted in most shops, restaurants, etc. Consequently, also quite young children need to have access to bank-cards and other digital payment solutions (Swish). This has contributed to a rather intense debate on 'data as a commodity',[40] its consequences and risks.

A considerable part of the on-going debate relates to security in different forms, that is the protection of data and information. However, the issue of personal data as payment

36 Datainspektionen beslut 1730-2014.
37 The Sundsvall Administrative Court of Appeal, case 719-04 and 761-04, judgement 4 June 2004.
38 The Stockholm Administrative Court of Appeal, case 7262-14, judgement 12 January 2015. It should be noted that this finding has been questioned.
39 The Gothenburg Administrative Court of Appeal, case 7074-15 and 165-16, judgement 23 March 2016.
40 Personal data has in the debate often been referred to as "the new oil".

is also part of these discussions. The Swedish Consumer Agency published a report on 'personal data as payment methods' from a consumer perspective.[41] The report states as a starting point that personal data have an economic value in real terms. In fact, it is a central part of the digital economy. Thus, it must be analyzed from a consumer rights' perspective. However, most consumer protection is directed towards the relationship business – consumer, which leads to the exclusion of many actors within the more network constructed Internet based eco-system.[42]

In the National Integrity Report 2019, the NSA found that some of the most common questions received by the authority concerned direct marketing and whether it is legal to use personal data for marketing purposes through mail and e-mail without the person's consent.[43]

It can thus be concluded that the debate is very much on-going.

Question 6

Article 22 GDPR gives the data subject the right not to be subjected to decisions based only on automated decision-making. This general principle is subject to a number of exemptions, one being national law. It follows from the Swedish Data Protection Act[44] that the principle shall not apply if it can be considered contrary to the Swedish Constitution, the Freedom of press Act[45] or the Fundamental Law on Freedom of Expression.[46] Furthermore, the principle shall not apply where personal data is processed for journalistic purposes or for academic, artistic or literary creation.[47]

In addition, the Swedish Administrative Act includes a general stipulation allowing for automated decision-making.[48] A cooperation between public authorities on the one hand, and the Swedish Association of Local Authorities and Regions (*SKR*) has interpreted this stipulation as an exemption from Article 22(2)(b) GDPR.[49]

Regarding safeguarding measures, the data subject should as a minimum level have the right to human intervention on the part of the controller to be able to articulate its stand point and to contest the decision.[50] The preparatory works to the previous Data Protection Act (the Personal Data Act) emphasize that as a starting-point the automated

41 Larsson, S and Ledendal, J, "Personuppgifter som betalningsmedel", Konsumentverket, KO, Rapport 2017:4.
42 *Ibid*, p. 10.
43 Nationell integritetsrapport 2019, Datainspektionens rapport 2019:2, p. 42.
44 Chapter 1, Section 7 Dataskyddslagen.
45 Tryckfrihetsförordning (1949:105).
46 Yttrandefrihetsgrundlag (1991:1469).
47 Chapter 1, Section 7, para. 2 Dataskyddslagen.
48 Section 28 Förvaltningslagen (2017:900).
49 eSam, uttalande 2018-03-19, see Öman, 2019, p. 370.
50 Öman, 2019, p. 371.

(contested) decision should be replaced by a new one in case where this is motivated and shown by the manual (human) re-view. However, there is no legal obligation to re-view the automated decision.[51]

Question 7

The so-called 'right to be forgotten' stipulated in article 17 GDPR may be considered extensive, but has in fact rather extensive exemptions. Under national Swedish law, the article cannot be applied in a manner that would restrict or prevent the principle on public access to official documents or the freedom of press, nor where personal data is processed for journalistic purposes or for academic, artistic or literary creation.[52] Furthermore, article 17 GDPR does itself contain a number of exemptions where the right to be forgotten does not apply.

Decisions under article 17 GDPR taken by an authority (including state, municipality and regional organization) may be challenged in administrative courts.[53]

The interpretation of the phrase 'erasure' has been discussed in Sweden. On a general level it should mean that the relevant personal data should be destroyed, that is deleted in a way so they cannot be recreated. In Swedish the term 'thin out' (*gallra*) is used.[54] In the preparatory works to the previous legislation, the Personal information Act, it was stated that personal data were not been erased in the meaning of the Data Protection Directive, if the data could be recreated using technical means and methods commonly accessible on the market.[55]

The right for the data controller *not* to erase personal data, has been addressed in a number of court-cases. For instance, the Supreme Administrative Court found that in case publicly accessible documents, which are required to be archived, include personal data, these personal data could not be erased.[56] The Administrative Court of Appeal came to the same conclusion in a case where the complainant requested his/her personal data to be erased from records in the County Court.[57]

51 SOU 1997:39 p. 405.
52 Chapter 1, Section 7 Dataskyddslagen.
53 Chapter 7, Section 2 Dataskyddslagen. This stipulation corresponds to what was previously Section 52 Personuppgiftslagen.
54 Öman, Sören, Dataskyddsförordningen (GDPR) m.m. En kommentar, Ed 1:1, Norstedts Juridik 2019, p. 333.
55 SOU 1997:39 p. 400.
56 Supreme Administrative Court, case no 5437-18, judgment 13 February 2019.
57 Administrative Court of Appeal of Stockholm, case no 10328-18, judgment 7 March 2019.

Question 8

Freedom of expression is guaranteed by the Swedish constitution[58], as has been described above (see Question 6). The National Swedish Data Protection Act excludes application of the GDPR in case it would be contrary to the Swedish constitution the Freedom of press Act or the constitution the Fundamental Law on Freedom of Expression.[59] The stipulation expressly states that articles 5-30 and 35-50 of GDPR and Chapter 2-5 the Data Protection Act, shall not apply to processing of personal data for journalistic purposes or for academic, artistic or literary creation.[60] There is extensive court practice concerning the interpretation and limits of 'journalistic purposes'. In summary can be said that publication I of information on the Internet with the aim to inform, criticize and create debate on current issues of interest to the general public, has been considered as 'journalistic purposes'. On the other hand, the Supreme Court has found that publication of information of purely private or personal character could normally not be considered as having 'journalistic purposes' even where the publication would be in a context that has 'journalistic purposes, in other respects.[61]

C Domestic Enforcement of Data Protection Law

Question 9

Sweden was the first country in the world to set up a NSA, the *Datainspektionen*, which was established in 1973. Its task was to safeguard the world's first Data Protection Act, entering into force that same year.[62] Consequently, the *Datainspektionen*, has considerable experience as the surveillance authority for data protection in Sweden.

Presently the *Datainspektionen* has about 80 members of staff, most of whom are lawyers. It is led by the Director-General, who is (as every Director-General of a Swedish authority) appointed by the government. The other positions are appointed following a standard recruitment process.

In addition to being the supervisory authority under the GDPR, the Swedish Data Protection Authority, is also Sweden's national supervisory authority regarding processing of personal data under the Schengen Convention, that is to say the convention on the EU's customs information systems, the Decision of the Council on the establishment of the EU

58 Yttrandefrihetsgrundlag (1991:1469).
59 Chapter 1, Section 7, para 1 Dataskyddslagen, see above Question 6.
60 Chapter 1, Section 7, para 2 Dataskyddslagen.
61 See for instance the Supreme Court's so-called "Ramsbro Judgement", NJA 2001 p. 409.
62 Datalag (1973:289).

Agency for law enforcement cooperation (Europol), the VIS Regulation, and the Eurodac Regulation.[63]

The *Datainspektionen* has a wide range of tasks. Its main fields of activity can be summarized as follows.

- Information: disseminating information and providing advice is an important part of the *Datainspektionen*'s tasks.
- Complaints, inquiries and tips: following up on complaints and carrying out inquiries into the application of the legislation for which Datainspektionen exercises supervision.
- Inspections: carrying out checks that laws and regulations are complied with through its own observations of companies, authorities and organizations. This is done through visits or by letter, phone or e-mail. Inspections are mostly planned, but can also be made following complaints or tip-offs from individuals or reports in the media.
- Legislative work: drawing up its own statutes with general regulations and publishing general guidelines with recommendations.
- Permits – issuing permits for companies to carry on debt recovery and credit rating activities. It should be noted that permits are not required to process personal data.

Datainspektionen's task and powers are stipulated in the *Dataskyddslagen*.[64]

Question 10

During the period 25 May 2018 to 23 April 2019, the Swedish NSA, the *Datainspektionen* received around 3,100 complaints concerning data protection. Around 80 per cent of these complaints concern private actors.[65]

The *Datainspektionen* is not obliged to act on a tip or a complaint. The decision whether to open an investigation and carry out an inspection depends among others on:

- whether it is a matter of a recurrent and systematic breach of regulations
- if there are serious shortcomings
- if it is a single case or a general breach of regulations
- if it is something that the *Datainspektionen* has already investigated.[66]

The *Datainspektionen* emphasizes the importance for any individual who suspects that his/her personal data is being processed in a way that does not comply with the GDPR, to

63 See for more information Datainspektionen's homepage: www.datainspektionen.se.

64 Chapter 6, Section 1 Dataskyddslagen.

65 These were complaints under the GDPR, the Criminal Data Act, the Camera Surveillance Act and the former Camera Surveillance Act. Nationell integritetsrapport 2019, Datainspektionens rapport 2019:2, p. 45.

66 See Datainspektionen's homepage: www.datainspektionen.se.

always try to resolve the problems themselves first. People are advised to contact the data processor with their concern and to follow-up to see what action has been taken to rectify non-compliant behaviour.[67]

Decisions by the *Datainspektionen* can be appealed, in which case the *Datainspektionen* will become party to the proceedings.[68] As the standing of the *Datainspektionen* in court cases on the appeal against its decisions has remained unchanged in subsequent legislation, the case law in which the *Datainspektionen* has acted as a party is extensive.

Question 11

At the time of writing of this national report, the *Datainspektionen* had issued only two decisions imposing fines.

The first case concerned a school in northern Sweden that had conducted a pilot using facial recognition to keep track of students' attendance in school. The test run was conducted in one school class for a limited period of time. The *Datainspektionen* found that the test violated several articles in GDPR.

The school had processed sensitive biometric data unlawfully and failed to do an adequate impact assessment, including seeking prior consultation with the *Datainspektionen*. The school had based the processing on consent, but the *Datainspektionen* considered that consent was not a valid legal bases given the clear imbalance between the data subject and the controller.[69]

The *Datainspektionen* imposed a fine on the municipality of approximately 20,000 euro. In Sweden, public authorities can receive a maximum fine of 10 million SEK (approximately 1 million euro).[70] The fine issued in this case, was the first one imposed by the *Datainspektionen*. The decision has been appealed and the case is pending.

The second case concerned a credit information site, called www.mrkoll.se.[71] On that web-site the company Nusvar AB published various information, including economic and financial information about all Swedish citizens above the age of 16. The aim of the site is to present official information of general interest concerning private individuals, such as for example social security number, housing situation, possession of vehicles, certain legal information and some information that is not public which may include telephone number. Further, the web-site contained economic and financial information that including

67 *Ibid.*
68 Chapter 7 Section 3 Dataskyddslagen. See Öman, Sören, Dataskyddsförordningen (GDPR) m.m. En kommentar, Ed 1:1, Norstedts Juridik 2019, p. 730 f.
69 Datainspektionen Decision, 20 August 2019, Reference number DI-2019-2221.
70 Chapter 6, Section 2, para 2 Dataskyddslagen.
71 Datainspektionen Decision, 13 December 2019, Reference number DI-2018-22737.

information on payment defaults. Such information was clustered in groups of 22-28 persons. In addition Nusvar AB also published information gathered from a large number of courts, including information on criminal charges and judgements.

In its decision Datainspektionen found that Nusvar AB had processed personal data contrary to articles 5 and 10 the GDPR. The fact that information was published about all Swedes above the age of 16, around 8 million people was considered aggravating circumstances, as well as the fact that information about criminal charges and judgements were published in connection with information of payment defaults. As Nusvar AB was a newly started undertaking, Datainspektionen estimated the turnover to at least 4,8 MSEK. Based on this the fine was set to 35,000 euro.

Question 12

Article 82 GDPR is the successor of article 23 of the Data Protection Directive.[72] In Sweden there has been a number of cases under the previous statute implementing that Directive.[73] It should be pointed out that questions of damages are dealt with under national tort law. In general, a data subject will be granted cost-recovery in case of damage as a result of data breaches. However, damages for intangible harm have been kept low. By way of example, the following cases can be mentioned. In a case where a person online named five persons, accusing them of rape, damages of 5,000 SEK (ca. 500 euro) were awarded.[74] In another case, a person had published a summary of a criminal judgment on Facebook, which resulted in the award of damages of 15,000 SEK (ca. 1,500 euro).[75] Even if examples of higher damages can be found, generally the amount of damages in Sweden is relatively low.

Question 13

The possibility for data subjects to be represented by an organization does not seem to be commonly used in Sweden. Under Swedish law, the data subject does retain standing as a party in such proceedings. Hence the data subject will have to issue a power of attorney

72 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

73 Personuppgiftslagen (1998:204).

74 District Court of Helsingborg (Helsingborgs tingsrätt), case no B 3915-00, Judgment 31 January 2001.

75 District Court of Mora (Mora tingsrätt), case no B 26-16 Judgment 9 September 2016.

in favour of the organization representing it. There is also a risk that the data subject would be (at least partly) responsible for any litigation costs.[76]

Question 14

Datainspektionen emphasizes its European co-operation, such as, for example, its participation in the European Data Protection Board (EDPB). Furtherit participates in co-operation within Schengen, Visa Information System (VIS) and Eurodac.

Concerning participation in the legislative process, Datainspektionen submits opinions in a large number of consultative statements which become part of the preparatory works. These statements are especially focusing on the issue that personal privacy is protected effectively. Further, Datainspektionen draws up its own statutes with general regulations and publishes general guidelines with recommendations on various issues. Datainspektionen also reviews drafts of statutes, requests for comment from the council on legislation and government bills, and sits on expert commissions and committees.[77]

D Data Processing for National Security Purposes

Question 15

Directive 2016/680/EC, is implemented into Swedish law by the *Brottsdatalagen*.[78] 'National security' is excluded from its application, both national security handled by the police, as well as national security handled by the military.[79]

Following the *Tele2 and Watson* judgments, the Swedish government issued an investigation. Following the legislative process, the national Swedish laws on storage and access to information on electronic communication in relation to crime-fighting, have been adjusted to EU legislation. The new stipulations entered into force 1 October 2019.[80]

76 Öman, Sören, Dataskyddsförordningen (GDPR) m.m. En kommentar, Ed 1:1, Norstedts Juridik 2019, p 578.

77 See Datainspektionen's homepage: www.datainspektionen.se.

78 Brottsdatalag (2018:1177).

79 Chapter 1, Section 4 Brottsdatalagen.

80 Lag om ändring i lagen (2003:389) om elektronisk kommunikation, Lag om ändring i lagen (2017:718) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, and Lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Switzerland

Jacques Beglinger[*]

Einleitung

Im föderativen Staatssystem der Schweiz ist der Datenschutz auf mehreren staatlichen Ebenen geregelt. Für den Umgang mit Personendaten wichtige Grundsätze finden sich bereits in der Schweizer Bundesverfassung (BV),[1] z. B. in Art. 13 BV (Schutz der Privatsphäre) und Art. 27 BV (Wirtschaftsfreiheit). Die Einzelheiten hierzu sind im Wesentlichen in dem im Jahr 1992 geschaffenen Bundesgesetz über den Datenschutz (DSG 1992),[2] in der dazugehörigen Verordnung (VDSG)[3] sowie in ergänzenden Empfehlungen und dergleichen (sog. *soft law*) geregelt. Hinzu kommt das neue Schengen-Datenschutzgesetz[4] (dazu unten Frage 1.1). Im Bereich des öffentlichen kantonalen Rechts gelten zudem kantonale Bestimmungen (auf welche in diesem Bericht jedoch nicht eingegangen wird).[5]

Auf der internationalen Ebene war die Europarats-Datenschutzkonvention No. 108 (im Folgenden: Europaratskonvention 108) für die Schweiz das erste rechtsverbindliche internationale Instrument im Bereich des Datenschutzes (für die Schweiz verbindlich seit dem 1.2.1998).[6] Sie stellt für das schweizerische Recht auch heute noch den wichtigsten internationalen Referenzpunkt dar. Die Konvention wurde von 2011 bis 2018 inhaltlich modernisiert (im Folgenden: Europaratskonvention 108+).[7] Nach anfänglichem Abwarten

---

* Lic. iur. Rechtsanwalt, Zürich/Bern. Der Verfasser dankt seiner Assistentin Carla Bertossa, MLaw, für die kompetente Mitarbeit.

1 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV), SR 101.

2 Bundesgesetz über den Datenschutz vom 19.6.1992 (DSG), SR 235.1.

3 Verordnung zum Bundesgesetz über den Datenschutz vom 14.6.1993 (VDSG), SR 235.11.

4 Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz) vom 28.9.2018 (SDSG), SR 235.3.

5 Zum geltenden Schweizer Datenschutzrecht in der Schweiz siehe etwa David Rosenthal/Yvonne Jöhri, *Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen*, 2. Auflage, Zürich: Schulthess 2018; Bruno Baeriswyl/Kurt Pärli (Hrsg.), *Stämpflis Handkommentar zum Datenschutzgesetz (DSG)*, Bern: Stämpfli 2015; Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), *Basler Kommentar. Datenschutzgesetz, Öffentlichkeitsgesetz*, 3. Auflage, Basel: Helbing Lichtenhahn 2014 sowie Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, *Datenschutzrecht. Grundlagen und öffentliches Recht*, Bern: Stämpfli 2011.

6 Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SEV Nr. 108, für die Schweiz SR 0.235.1.

7 Änderungsprotokoll zu dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 18. Mai 2018, SEV Nr. 223; siehe hierzu www.coe.int/de/web/conventions/full-list/-/conventions/treaty/223?_coeconventions_WAR_coeconventionsportlet_languageId=en_GB

beschloss der Schweizer Bundesrat (Bundesregierung) am 30.10.2019 die Unterzeichnung[8], welche am 21.11.2019 beim Europarat in Strassburg hinterlegt wurde[9]. Mit der Überweisung an das Parlament am 6.12.2019 leitete der Bundesrat sodann umgehend das Ratifikationsverfahren in die Wege.[10] Bereits am 23.1.2020 stimmte die wichtige Fachkommission des Nationalrats der Genehmigung der Konvention deutlich zu.[11] Damit wird u.a. die Signalwirkung angestrebt, dass die Schweiz die internationale Erhöhung des Datenschutz-Standards mittragen will.[12]

Vor diesem Hintergrund sowie angesichts der Neuerungen im EU-Datenschutzrecht (dazu sogleich im Rahmen der Beantwortung der Fragen) befindet sich das schweizerische Datenschutzrecht derzeit in einem grundlegenden Erneuerungsprozess. Dieser Bericht zielt insbesondere darauf, die gestellten Fragen im Licht der *künftigen* Rechtslage in der Schweiz zu beantworten, soweit dies im Zeitpunkt der Schriftlegung (letzte Anpassungen am 12.2.2020) und in Anbetracht der Unwägbarkeiten des noch laufenden politischen Prozesses möglich ist.

---

sowie Council of Europe, *Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data*, Strasbourg: Council of Europe 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Hinweis: Die Fundstellen der Online-Quellen wurden zuletzt am 12.2.2020 besucht.

8 Für die Ankündigung siehe Protokoll Nationalrat 24.9.2019, Votum 14, www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=47356#votum14. Zum Beschluss des Bundesrates siehe die Medienmitteilung vom 30.10.2019: Datenschutzkonvention des Europarates: Bundesrat beschliesst Unterzeichnung, www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2019/2019-10-30.html.

9 Council of Europe, Chart of signatures and ratifications of Treaty 223, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.

10 Medienmitteilung Bundesrat: Datenschutzkonvention des Europarates: Bundesrat verabschiedet Botschaft; https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2019/2019-12-061.html#moreinfos-tab-1. Botschaft: Botschaft zur Genehmigung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten; https://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2019/2019-12-061/bot-d.pdf.

11 Medienmitteilung der Staatspolitischen Kommission des Nationalrats (SPK-NR) vom 24.1.2020: "Grünes Licht für die Ratifizierung des Datenschutzübereinkommens des Europarates. Die SPK-NR hat sich mit 19 zu 6 Stimmen für das Protokoll zur Änderung des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108+) ausgesprochen (19.068). Damit beantragt sie ihrem Rat, den Bundesrat zur Ratifizierung dieses Instruments zu ermächtigen.", https://www.parlament.ch/press-releases/Pages/mm-spk-n-2020-01-24.aspx.

12 Medienmitteilung des Bundesrat vom 30.10.2019 (Fn. 8): "Mit der Unterzeichnung bekennt sich die Schweiz zu einem international anerkannten Datenschutzstandard […]." Siehe weiter ausführlich Jacques Beglinger, Fragen & Antworten zur modernisierten Datenschutzkonvention 108 des Europarats und zur EU-Datenschutzäquivalenz, Ausgabe 2019-12.1, Online-Publikation, Bern: SwissHoldings, abrufbar unter https://swissholdings.ch/dossier-datenschutzrevision, Frage 28 ff.

A Setting the Scene – Weichenstellung

Frage 1

Relevanz des EU-Datenschutzrechts für das Schweizer Recht

Die Schweiz nimmt in ihrem europäischen Umfeld eine besondere Stellung ein: Sie ist zwar Mitgliedstaat der Europäischen Freihandelsassoziation (EFTA), nicht aber des Europäischen Wirtschaftsraums (EWR).[13] Stattdessen setzt die Schweiz in ihrem Verhältnis zur EU den bereits in den 1950er Jahren eingeschlagenen Weg der sog. bilateralen (vornehmlich schweizerische Terminologie) bzw. sektoriellen (vornehmlich EU-Terminologie) Abkommen fort.[14]

Die in der Fragestellung erwähnte Sekundärgesetzgebung der EU ist zwar vollumfänglich für den EWR relevant, nicht aber in gleichem Masse für das bilaterale Recht zwischen der Schweiz und der EU. Unmittelbare rechtliche Berührungspunkte bestehen nur zum Teil, insofern als die Thematik von den Schengen-[15] und Dublin-Assoziationsabkommen[16] erfasst wird.[17] Via diese Abkommen ist die EU-Richtlinie 2016/680[18] auch für die Schweiz relevant.[19] Im Revisionsprozess des Schweizer DSG wurde dieser Teil zeitlich vorgezogen.

---

13 Zur Rolle der Schweiz in der Entstehungsgeschichte des EWR siehe insbesondere Philippe G. Nell, *Suisse-Communauté Européenne. Au coeur des négotiations sur l'Espace économique européen*, Paris: Economica 2012; Dieter Freiburghaus, *Königsweg oder Sackgasse? Schweizer Europapolitik von 1945 bis heute*, 2. überarbeitete Auflage, Zürich: Verlag Neue Zürcher Zeitung 2015.

14 Zum Ganzen siehe etwa Matthias Oesch, *Europarecht. Band I: Grundlagen, Institutionen, Verhältnis Schweiz-EU*, 2. Auflage, Bern: Stämpfli 2019; Thomas Cottier et al., *Die Rechtsbeziehungen der Schweiz und der Europäischen Union*, Bern: Stämpfli 2014, sowie Christa Tobler/Jacques Beglinger, *Grundzüge des bilateralen (Wirtschafts-)Rechts. Systematische Darstellung in Text und Tafeln*, 2 Bände (Text und Tafeln), Zürich/St. Gallen: Dike 2013.

15 Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, für die Schweiz SR 0.362.31, für die EU und die EG (heute nur noch die EU), ABl. 2008 L 53/52.

16 Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags, für die Schweiz SR 0.142.392.68, für die EG (heute die EU) ABl. 2008 L 53/5.

17 Hierzu Jacques Beglinger, ‚Die Schweiz und der (digitale) EU-Binnenmarkt – Swiss country report', in: The internal market and the digital economy, Proceedings FIDE Congress 2018 vol.1, Coimbra: FIDE, 2018, S. 768 f., mit weiteren Hinweisen.

18 Richtlinie 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119/89.

19 Hierzu die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 S. 6991 ff., https://www.admin.ch/opc/de/

Das daraus resultierte Schengen-Datenschutzgesetz (SDSG)[20] ist am 1.3.2019 in Kraft getreten.

Im Gegensatz dazu ergibt sich für die EU-Verordnung 2016/679[21] (Datenschutzgrundverordnung, DSGVO) eine Verbindlichkeit für die Schweiz nicht aus den erwähnten Abkommen mit der EU.[22] Nach der Auffassung der Bundesbehörden erfolgt die jetzt laufende Anpassung des Schweizer Rechts an die DSGVO deshalb unabhängig von abkommensrechtlichen Verpflichtungen im Weg des sog. autonomen Nachvollzugs, um so die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der DSGVO anzunähern.[23] Diese Strategie der einseitigen Anpassung des Schweizer Rechts an ausgewähltes EU-Recht zielt darauf, den Wirtschaftsaustausch auch ausserhalb von formellen Abkommen zu erleichtern.[24]

Angemessenheitsregime

Die soeben erwähnte Strategie des autonomen Nachvollzugs will weiter erreichen, dass die Schweiz die im internen EU-Recht für Drittstaaten vorgesehene Angemessenheits- bzw. (nach schweizerischer Terminologie) Äquivalenzanerkennung gemäss Art. 45 DSGVO beibehalten kann.[25] Dabei geht es um die Angemessenheit der Schweizer Datenschutzniveaus, wobei gemäss Erwägung 105 in der Präambel der DSGVO der Standard der Europaratskonvention 108 bzw. 108+ ein wesentliches Element darstellt:

> Insbesondere sollte der Beitritt des Drittlands zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den Ausschuss

---

federal-gazette/2017/6941.pdf. Nach schweizerischer Terminologie wird der einen Regierungsentwurf begleitende erläuternde Bericht zuhanden des Parlaments als „Botschaft" bezeichnet.

20 Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG), SR 235.3.

21 Verordnung 2016/679/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/8.

22 Hierzu Botschaft (Fn. 19), S. 6998. Anderer Auffassung Astrid Epiney, ‚Verweise auf EU-Sekundärrecht im Bilateralen Recht. Zur Reichweite von Verweisen auf EU-Sekundärrecht in den Bilateralen Abkommen bei der Weiterentwicklung des Unionsrechts', *Jusletter* 11. September 2017.

23 Hierzu etwa Walter A. Stoffel/Claudia Seitz, ‚Autonomer Nachvollzug – Das Wirtschaftsrecht der Schweiz zwischen Angleichung und Eigenständigkeit', *Europäische Zeitschrift für Wirtschaftsrecht* 2012, 841-843.

24 Die DSGVO entfaltet in praktischer Hinsicht in der Schweiz bereits Wirkung, indem sie nicht nur Sachverhalte innerhalb der EU, sondern geographisch auch darüber hinaus erfasst, also auch in der Schweiz (Umschreibung des räumlichen Anwendungsbereichs nach Art. 3 DSGVO).

25 Ausführlich Beglinger, Fragen & Antworten (Fn. 12), Frage 49 ff.

> konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet.[26]

Im Rahmen des früheren EU-Rechts (Richtlinie 95/46)[27] liegt für die Schweiz eine Äquivalenzentscheidung der Europäischen Kommission aus dem Jahr 2000 vor.[28] Hier stellen die neuen Regelungen der DSGVO für den Schweizer Rechtsrahmen Herausforderungen dar, welche massgeblich zur nun laufenden Revision des Schweizer Datenschutzrechtes geführt haben:[29]

> "Künftig wird die schweizerische Gesetzgebung anhand der in der Verordnung (EU) 2016/679 enthaltenen Anforderungen überprüft. Falls die Schweiz den Angemessenheitsbeschluss beibehalten bzw. im Falle eines Widerrufs erneut eine Bestätigung über das angemessene Datenschutzniveau erreichen möchte, ist es insbesondere für die Wirtschaft von zentraler Bedeutung, dass die schweizerische Gesetzgebung einen den Anforderungen dieser Verordnung entsprechenden Schutz gewährleistet."

Zu ergänzen bleibt, dass die Angemessenheit namentlich auch für Forschung und Entwicklung an den Hochschulen von zentraler Bedeutung ist.

Nicht zuletzt vor diesem Hintergrund hat der schweizerische parlamentarische Prozess jüngst eine starke Beschleunigung erfahren.[30] Zugleich hat sich politisch die Ansicht durchgesetzt, dass sich der Schweizer Datenschutz inhaltlich den EU-Regeln weitgehend annähern soll.[31] Zusammen dürfte dies ermöglichen, dass die EU-Kommission in der

---

26 Siehe neuestens auch Medienmitteilung des Bundesrats vom 30.10.2019 (Fn. 9): "Schliesslich kommt ihr [d.h. Europaratskonvention 108+] auch im Rahmen der anstehenden Angemessenheitsprüfung des schweizerischen Datenschutzniveaus durch die EU grosse Tragweite zu: Die EU berücksichtigt bei ihrem Entscheid jeweils, ob die entsprechenden Drittstaaten der Konvention beigetreten sind."

27 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281/31 (in der EU nicht mehr in Kraft).

28 Entscheidung 2000/518/EU gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl. 2000, L 215/1.

29 So der Bundesrat in der Botschaft (Fn. 19), S. 6943.

30 Siehe etwa *Neue Zürcher Zeitung*, Weil ein Konflikt mit der EU droht – der Ständerat gibt beim Datenschutz Gas, 24.10.2019, https://www.nzz.ch/schweiz/datenschutz-staenderat-beschleunigt-um-konflikt-mit-eu-zu-meiden-ld.1516350; Staatspolitische Kommission Ständerat, Medienmitteilung, 25.10.2019: Kommission unterbreitet dem Rat Transparenz-Initiative mit indirektem Gegenvorschlag, https://www.parlament.ch/press-releases/Pages/mm-spk-s-2019-10-25.aspx: „Die Kommission hat die Beratungen zur Totalrevision des Datenschutzgesetzes (DSG) (17.059) aufgenommen und hat das Eintreten einstimmig beschlossen. Da es ihrer Ansicht nach gilt, möglichst rasch Rechtssicherheit zu schaffen im Hinblick auf die Äquivalenz zu den Regelungen in der EU, behandelt sie das DSG in diesem Quartal prioritär […]".

31 SDA-Meldung zur Behandlung im Ständerat als Zweitrat, 18.12.2019: "Ständerat ist bei der Revision des Datenschutzgesetzes auf EU-Linie – Der Ständerat will den Schutz persönlicher Daten verstärken und die Regeln für sogenanntes Profiling verschärfen. Bei der Revision des Datenschutzgesetzes weicht er damit

aktuellen Überprüfung der Angemessenheit betreffend die Schweiz bereits auf eine politisch gefestigte Regulierungslage «post Revision» abstellen kann.

Frage 2

Der schweizerische Datenschutz beruht, zumindest betreffend die Bearbeitung von Personendaten durch Private, im Wesentlichen auf dem Schutz der Persönlichkeit gemäss Art. 27 ff. Zivilgesetzbuch (ZGB).[32] Auf der Ebene der Bundesverfassung sind weiter der Schutz der Privatsphäre nach Art. 13 BV sowie die Wirtschaftsfreiheit nach Art. 27 BV relevant.

Mit der Anpassung des DSG und weiterer Erlasse des schweizerischen nationalen Rechts an internationale Datenschutzstandards, namentlich an die Europaratskonvention 108+ und an die EU-DSGVO, erfährt der Schweizer Datenschutz zunehmend eine über diese Grundsätze hinausgehende, erweiterte Prägung.

Da die Schweiz der EU nicht angehört, ist für sie die EU-Grundrechtecharta nicht anwendbar.[33] Hingegen gilt in der Schweiz die Europäische Menschenrechtskonvention (EMRK),[34] welche in Art. 8 – gleich wie Art. 7 EU-Grundrechtecharta – das Recht auf Achtung des Privatlebens schützt. Die EMRK enthält jedoch, anders als Art. 8 EU-Grundrechtecharta, keine explizite Bestimmung betreffend den Schutz der personenbezogenen Daten. Jedoch wurde namentlich aus dem Gedanken des Schutzes

---

von verschiedenen Beschlüssen des Nationalrats ab. Das Ziel sind EU-kompatible Regeln.", https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059, sowie Medienmitteilung Staatspolitische Kommission des Nationalrats, 24.1.2020: "Nach der Erstberatung durch die beiden Räte wird nun das Differenzbereinigungsverfahren zur Totalrevision des Datenschutzgesetzes […] durchgeführt. Die Staatspolitische Kommission des Nationalrates (SPK-NR) beantragt ihrem Rat, in mehreren wichtigen Punkten dem Ständerat zu folgen, […]", https://www.parlament.ch/press-releases/Pages/mm-spk-n-2020-01-24.aspx.

32 Die entsprechenden spezifischen Artikel sind seit dem 1. Juli 1985 in Kraft (AS 1984 778; BBl 1982 II 636). Vgl. auch Frank Seethaler, ‚Entstehungsgeschichte des Datenschutzgesetzes', in: Basler Kommentar DSG (Fn. 5), N 34 ff.

33 Anderer Meinung Epiney, welche die Auffassung vertreten, dass die EU-Grundrechte via bestimmte bilaterale Abkommen bzw. via darin erwähntes EU-Recht auch in der Schweiz beachtet werden müssen; Astrid Epiney, 'Zur Verbindlichkeit der EU-Grundrechte in der und für die Schweiz', in: Bernhard Altermatt/Gilbert Casasus (Hrsg.), *50 Jahre Engagement der Schweiz im Europarat 1963-2013. Die Schweiz als Akteur oder Zaungast der europäischen Integration?*, Zürich: Somedia 2013, 141-158; Matthias Oesch/Tobias Naef, ‚EU-Grundrechte, der EuGH und die Schweiz', Zeitschrift für Schweizerisches Recht 2017 I, 117-144. Oesch (S. 135 ff.) weist zudem darauf hin, dass die EuGH-Rechtsprechung zu *Safe Harbour* die *Privacy Shield*-Regelung Schweiz-USA beeinflusst hat.

34 In Kraft getreten für die Schweiz am 28. November 1974; https://www.admin.ch/opc/de/classified-compilation/19500267/index.html.

des Privatlebens und weiter der Freiheit der Meinungsäusserung gemäss Art. 10 EMRK[35] die Idee des Datenschutzes entwickelt, die sodann in der Europaratskonvention 108 ihren Niederschlag fand.

Die Annahme von materiell-rechtlichen DSGVO-Vorschriften in der nationalen Rechtsordnung

Nachdem in der Schweiz die gesetzliche Annäherung an die DSGVO noch in Vorbereitung ist, besteht hierzu noch keine Praxis. Wo möglich, wird im Folgenden aber auf die voraussichtlich künftige Gesetzeslage hingewiesen, wie sie sich im Zeitpunkt der Schriftlegung darbietet. Die folgenden Hinweise hierzu beziehen sich auf den Entwurf zur Totalrevision DSG, wie er am 15.9.2017 vom Bundesrat zusammen mit einem erläuternden Bericht (sog. «Botschaft») verabschiedet wurde.[36] Der Entwurfstext wird im Folgenden als E-DSG bezeichnet. Er befindet sich zur Zeit in der parlamentarischen Beratung. Mit dem Abschluss der Parlamentsarbeiten wird im Frühling oder Sommer 2020 gerechnet. Unter Umständen könnte das Gesetz anschliessend noch einem Referendum gemäss den Regeln der schweizerischen Direktdemokratie unterstehen.

B Die Annahme von materiell-rechtlichen DSGVO-Vorschriften in der nationalen Rechtsordnung

Frage 3

Nach schweizerischem Verständnis stellt die Verpflichtung zum Handeln nach Treu und Glauben eine Fundamentalnorm dar. Bereits Art. 5 Abs. 3 BV verlangt: «Staatliche Organe und Private handeln nach Treu und Glauben.» Dies gilt somit auch für den Datenschutz.

Art. 5 E-DSG nimmt unter dem Titel «Grundsätze» den Gedanken der Fundamentalnorm auf und fasst die verschiedenen Sätze – im Vergleich zum geltenden Art. 4 DSG in leicht erweiterter Form) zusammen:

> "Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein (Abs. 2). Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so

35 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in: Council of Europe, *Convention 108 +* (Fn. 7), ab S. 15, N 19. Siehe auch Seethaler (Fn. 32), N 10.

36 Bundesrat, Medienmitteilung, 15.9.2017: Den Datenschutz verbessern und den Wirtschaftsstandort stärken, https://www.bj.admin.ch/bj/de/home/aktuell/news/2017/ref_2017-09-150.html, mit Links zu den Gesetzesmaterialien.

> bearbeitet werden, dass es mit diesem Zweck vereinbar ist (Abs. 3). Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Abs. 4)."

Angesichts der Unbestimmtheit der Begriffe wird eine breite Auslegungstätigkeit der Behörden und Gerichte unumgänglich sein.[37]

Frage 4

De lege lata sind die neuesten richterlichen Erwägungen massgeblich im Leitentscheid des Schweizerischen Bundesverwaltungsgerichts *Moneyhouse* vom 18.4.2019 zusammengefasst:[38]

Nach Art. 4 Abs. 5 zweiter Satz DSG 1992 ist zur rechtmässigen Bearbeitung von Persönlichkeitsprofilen eine explizite Einwilligung der betroffenen Person notwendig. Gemäss dem Bundesverwaltungsgericht erfordert die Einwilligung, dass die betroffene Person in den Grundzügen über Gegenstand, Zweck und Umfang der beabsichtigten Datenbearbeitung aufgeklärt sein muss, damit sie die Konsequenzen der Einwilligung abschätzen kann. Die explizite Einwilligung muss nachwiesen werden; weder die persönliche Benutzererkennung noch die Angabe eines Interessensnachweises vermögen die Einwilligung der betroffenen Person zu substituieren. Im übrigen griff im vorliegenden Fall die gesetzliche Vermutung von Art. 12 Abs. 3 DSG, wonach keine Persönlichkeitsverletzung vorliegt, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat, so dass eine unbestimmte Zahl von Personen sie ohne wesentliche Hindernisse in Erfahrung bringen kann, ohne die Bearbeitung ausdrücklich zu verbieten, nicht. Hierfür wäre laut dem Bundesverwaltungsgericht erforderlich, dass die betroffene Person ihre Daten mit Wissen und Willen allgemein zugänglich gemacht hat oder durch einen Dritten zugänglich machen liess. Blosses Dulden der Handlung eines Dritten, ohne etwas zum Zugänglichmachen beizutragen, genügt indes nicht (*Moneyhouse*, E. 5.4.1).

Mit Bezug auf eine Rechtfertigung aufgrund von überwiegenden öffentlichen und privaten Interessen nach Art. 13 DSG weist das Bundesverwaltungsgericht darauf hin, dass öffentliche Interesse in der Praxis gegenüber den privaten Interessen immer eine untergeordnete Rolle spielen. Zum einen bestehen für öffentliche Interessen häufig gesetzliche Regelungen, die eine Datenbearbeitung auch ohne Interessenabwägung

37 Für Beispiele und Verweisungen siehe etwa Botschaft (Fn. 19), S. 7024 f.

38 Urteil des Bundesverwaltungsgerichts vom 18. April 2017 (A-4232/2015), EDÖB gegen Moneyhouse AG, https://jurispub.admin.ch/publiws/download?decisionId=29c591dc-a585-4b62-b2fa-8e4efca92f73. Siehe zur Thematik auch Tobias Fasnacht, *Die Einwilligung im Datenschutzrecht. Vorgaben einer völkerrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht*, Zürich: Schulthess 2017.

rechtfertigen, zum anderen liegt zumeist, wenn ein überwiegendes öffentliches Interesse gegeben ist, auch ein überwiegendes privates Interesse vor. Den privaten und öffentlichen Interessen, die für die Datenbearbeitung sprechen, sind die berechtigten Interessen der betroffenen Personen gegenüberzustellen; es ist folglich eine Interessenabwägung vorzunehmen (*Moneyhouse*, E. 5.4.2).

De lege ferenda werden die Umstände der „Einwilligung" und des Überwiegens „berechtigter Interessen" noch debattiert. Eine gesicherte Aussage ist deshalb nicht möglich.

Frage 5

Ein regulatorischer Niederschlag zur Verwendung von personenbezogenen Daten als „Gegenleistung" für die Bereitstellung von digitalen Inhalten ist in der Schweiz nicht auszumachen. In gesellschaftlicher Hinsicht wird eine entsprechende Diskussion jedoch unter dem Schlagwort der «Datensouveränität» geführt.[39]

Spezifisch im Pressewesen haben die grossen Schweizer Medienhäuser Tamedia, Ringier, CH Media und NZZ sowie die öffentliche Mediengesellschaft SRG im September 2019 angekündigt, dass sie kollektiv ab September 2020 eine Registrierung für alle Online-Inhalte einführen werden. «Durch die Registrierung erhalten die Medienhäuser zusätzlichen Daten von ihren Nutzern, was zielgenauere Werbung ermöglicht. Damit wollen die Verleger ihre Position im Wettbewerb mit den übermächtigen amerikanischen Technologiekonzernen Google und Facebook stärken».[40]

Frage 6

Die Verpflichtung zur Vermeidung von rein automatisierten Entscheidungen ergibt sich bereits aus Art. 9 Abs. 1 lit. a der Europaratskonvention 108+:

> Every individual shall have a right […] not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.

39 Vgl. etwa digitaleschweiz, Initiative für „Smart Switzerland", Leitbild „Datensouveränität" – Impulse für die Schaffung einer digitalen Privatautonomie, https://www.digitaleschweiz.ch/government/digitale-souveranitat-ein-handlungsfeld-fur-vertrauenbildung; Florent Thouvenin, Rolf H. Weber, Alfred Früh, Elemente einer Datenpolitik, Zürich: Schulthess 2019, S. 17, 32 ff.

40 *Tagesanzeiger* (Zürich), 19.9.2019, Login-Pflicht für Schweizer Mediennutzer, https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/loginpflicht-fuer-schweizer-mediennutzer/story/15481924.

De lege ferenda adressiert das E-DSG die Thematik in Art. 19 unter dem Titel «Informationspflicht bei einer automatisierten Einzelentscheidung». Die genauen Umstände der Nutzung automatisierter Entscheidung werden aber noch debattiert.[41] Eine gesicherte Aussage ist deshalb nicht möglich.

Frage 7

In Art. 28 Abs. 2 lit. c. E-DSG wird entsprechend den Anforderungen von Art. 8 lit. e Europaratskonvention 108+ ausdrücklich ein Klagerecht auf Löschung formuliert, ähnlich Art. 17 DSGVO. Dieses Recht auf Löschung entspricht im Bereich des Datenschutzes dem «Recht auf Vergessenwerden», wie es generell aus dem zivilrechtlichen Persönlichkeitsschutz abgeleitet wird. Der E-DSG führt demnach grundsätzlich die bisherige Rechtslage fort.[42]

Frage 8

Ein entsprechendes Gesetzgebungsvorhaben im autonomen Nachvollzug (dazu oben zu Frage 1) ist in der Schweiz nicht in Sicht.

C Nationale Durchsetzung von Datenschutzrecht

Frage 9

Im föderativen Datenschutzsystem der Schweiz ist die Aufsicht auf verschiedene staatliche Ebenen aufgeteilt. Im Anwendungsbereich des DSG 1992 wird sie gemäss Art. 26 ff. des Gesetzes durch den Eidgenössischen Datenschutz- und Öffentlichkeitsberater (EDÖB) ausgeübt. Auf kantonalem Niveau steht es den Kantonen frei, die Aufsicht eigenständig und damit potentiell unterschiedlich zu gestalten. In der Praxis folgen die Kantone jedoch in der Regel denselben Prinzipien.[43] Die kantonalen Datenschutzgesetze sehen jeweils ebenfalls eine Aufsichtsstelle vor.[44] Daneben ist auch eine Vielzahl von kommunalen Datenaufsichtsbehörden eingesetzt.

41 Vergleiche zum Aspekt, ob die Regulierung bereits beim Vorgang des Profilierens oder erst bei der Nutzung des einmal entstanden Profils ansetzen soll, Cornelia Stengel / Luca Stäuble, Vom Persönlichkeitsprofil zum Profiling mit hohem Risiko, *Jusletter* 20. Januar 2020.

42 Vgl. auch Botschaft (Fn. 19), S. 7077 f.

43 Siehe die Verweisungen zu den kantonalen Datenschutzgesetzen auf der Webseite von *privatim*, der Konferenz der schweizerischen Datenschutzbeauftragten, http://www.privatim.ch/de/privatim.

44 Idem für die Auflistung der kantonalen Aufsichtsbehörden.

Eine im Jahr 2011 erstellte offizielle Evaluation der Wirksamkeit des DSG 1992 wies auf Verbesserungsbedarf bei der Durchsetzung im Datenschutz hin. Zwar fehlt es nicht an den rechtlichen Instrumenten, die grundsätzlich denjenigen in Vergleichsländern ebenbürtig sind.[45] Jedoch werden die Durchsetzungsrechte zu wenig häufig beansprucht.[46] Deshalb folgerte der Bundesratsbericht, dass in einer künftigen Revision u.a. zu prüfen sei, ob die Aufsichtsmechanismen gestärkt und die Rechtsansprüche der Betroffenen sowie deren Durchsetzung an die aufgrund der technologischen Entwicklungen veränderten Verhältnisse angepasst werden sollten.[47]

Das E-DSG misst dementsprechend der Durchsetzung und Sanktionierung von Datenschutzverletzungen grosse Bedeutung zu. Dabei wird am dualen Durchsetzungs- und Sanktionsweg, an dessen grundsätzlicher Konzeption der Evaluationsbericht nichts auszusetzen hatte, festgehalten. Dieses setzt einerseits auf administrative Aufsicht durch den EDÖB, dem dafür die Kompetenz zu Verwaltungsmassnahmen (ohne Bebussung) gegeben und entsprechende Durchsetzungsmittel zur Verfügung gestellt werden. Andererseits sind Strafsanktionen gegen fehlbare Individualpersonen im ordentlichen Strafverfahren vorgesehen. Hinzu kommt, dogmatisch aber anders gelagert, noch die Schadensliquidation im Zivilverfahren. Damit erfüllt die Schweiz auch ihre internationale Verpflichtung zu geeigneten Sanktionen und Rechtsmitteln gemäss Europaratskonvention 108 bzw. künftig 108+.

Das E-DSG wird die Stellung der Aufsicht auf der nationalen Ebene, also des EDÖB,[48] nun verstärken:

> "Die Stellung und die Unabhängigkeit des Beauftragten werden gestärkt. Diese oder dieser kann zwei Mal wiedergewählt werden. Sie oder er darf nur unter ganz bestimmten Bedingungen einer Nebenbeschäftigung nachgehen. Im Weiteren sieht der E-DSG vor, dass der Beauftragte – wie seine Kolleginnen und Kollegen in den anderen europäischen Ländern – nach Abschluss einer Untersuchung, die von Amtes wegen oder auf Anzeige hin eingeleitet wurde, Verfügungen erlassen kann, die für die Verantwortlichen und die

45 Büro Vatter, *Evaluation des Bundesgesetzes über den Datenschutz, Schlussbericht*, Bern, 10.3.2011, https://www.ejpd.admin.ch/content/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf, S. 72 ff. Dieser Schlussbericht hielt auf S. 75 dazu sogar explizit fest: «Die Betroffenen von Datenbearbeitungen in der Schweiz sind somit bezüglich ihrer Durchsetzungsrechte ähnlich gut und teilweise sogar besser ausgestattet als die Betroffenen der im Rechtsvergleich untersuchten Staaten.»

46 Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, https://www.admin.ch/opc/de/federal-gazette/2012/335.pdf, S. 343.

47 Idem, S. 350.

48 Etwas verwirrend wird die Aufsichtsbehörde im Gesetzesentwurf personalisiert formell als «Eidgenössischer Datenschutz- und Öffentlichkeitsberater (EDÖB)» bezeichnet (Art. 3 E-DSG). Die individuelle Führungsperson an der Spitze der Behörde heisst demgegenüber formell «Beauftragte oder Beauftragter» (Art. 39 Abs. 1 E-DSG).

> Auftragsbearbeiter verbindlich sind. Nur das Bundesorgan bzw. die private Person, gegen das bzw. die die Untersuchung eingeleitet wurde, sind in einem Untersuchungsverfahren Partei."[49]

Der EDÖB beaufsichtigt die Anwendung der bundesrechtlichen Datenschutzvorschriften. Von dessen Aufsicht sind die Bundesversammlung, der Bundesrat, die eidgenössischen Gerichte, die Bundesanwaltschaft (aber nur betreffend die Bearbeitung von Personendaten im Rahmen von Strafverfahren) und weitere Bundesbehörden, soweit diese Personendaten im Rahmen einer rechtsprechenden Tätigkeit oder von Verfahren der internationalen Rechtshilfe in Strafsachen bearbeiten, befreit (Art. 3 E-DSG).

Die Bestimmungen zur Organisation des EDÖB und seinen Aufgaben sind im 7. Kapitel des Gesetzesentwurfs (Art. 39 ff. E-DSG) zusammengefasst. Zur Stärkung der Unabhängigkeit wird die Bedeutung des Parlaments (Vereinigte Bundesversammlung) bei der Organisation erhöht. So wird der Leiter des EDÖB nicht mehr – wie unter dem DSG 1992 – vom Bundesrat als Exekutivorgan, sondern neu vom Parlament gewählt (Art. 39 Abs. 1 E-DSG); dieses entscheidet auch über eventuelle Bewilligung zur Ausübung von Nebenämtern (Art. 41 Abs. 2 E-DSG). Zudem unterbreitet der EDÖB neu sein Budget ebenfalls dem Parlament und nicht mehr der Exekutive (Art. 40a E-DSG). Damit werden auch verschiedene Verpflichtungen gemäss Art. 15 der Europaratskonvention 108+ eingelöst.

In den Aufgabenkreis des EDÖB fällt namentlich die Untersuchung von Verstössen gegen Datenschutzvorschriften (Art. 43 E-DSG). Hierzu stehen ihm im Wesentlichen dieselben Befugnisse wie den Untersuchungsbehörden im gerichtlichen Verfahren zu, insbesondere auch der Zugang zu allen relevanten Unterlagen sowie zu Räumlichkeiten und Anlagen, falls notwendig auch unter Beizug der Polizeiorgane (Art. 44 E-DSG). Er kann ferner Verwaltungsmassnahmen ergreifen (Art. 45 E-DSG). Allerdings soll dem EDÖB weiterhin keine Kompetenz zum Erlass von Verwaltungssanktionen zukommen; dies im Gegensatz zu vergleichbaren europäischen Behörden. Als Ausgleich dafür werden aber – wie bereits erwähnt – die Strafbestimmungen massgeblich verschärft und insbesondere das Missachten der Verfügungen des Beauftragten mit Busse bedroht.[50] Siehe zum Sanktionensystem im E-DSG ausführlicher hinten ab Frage 11.

49 Botschaft (Fn. 19), S. 34 f.

50 Botschaft (Fn. 19), S. 6973 f. (1.4.2.5).

Frage 10

Der EDÖB eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Er kann jedoch von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist (Art. 43 Abs. 1 und 2 E-DSG). Daneben verpflichtet ihn das Gesetz, auf die Sensibilisierung der Bevölkerung in Bezug auf den Datenschutz hinzuwirken (Art. 52 Abs. 1 Bst. c E-DSG). Die Wahl der Strategie beim Aufgreifen und bei der Behandlung von Beschwerden liegt im Ermessen des EDÖB.[51]

Frage 11

Der schweizerische Datenschutz sieht bereits vor der Revision wirksame Durchsetzungsmechanismen vor, dies auch, um den im Rahmen der Europaratskonvention 108 eingegangenen Verpflichtungen zu genügen.[52] Die schweizerische Datenschutzkonzeption wird auch künftig grundsätzlich von einem – allerdings deutlich verschärften – Strafsystem ausgehen, welches sich markant vom System von den finanziellen Verwaltungssanktionen der DSGVO unterscheidet (zum Letzteren siehe unten betreffend späteren Systemwechsel).

DSG 1992 – Sanktionen im Datenschutzrecht de lege lata

Strafbestimmungen
Sanktioniert wird die Verletzung der im DSG statuierten Auskunfts-, Melde- und Mitwirkungspflichten (Art. 34 DSG 1992) sowie die Verletzung der beruflichen Schweigepflicht (Art. 35 DSG 1992). Bei den Strafbestimmungen im DSG handelt es sich um Nebenstrafrecht.[53] Das heisst, die allgemeinen Bestimmungen des Strafgesetzbuches (StGB)[54] finden Anwendung, sofern im DSG 1992 keine Sonderregelung besteht.[55] Da

51 Siehe zur aktuellen Schwerpunktsetzung 26. *Tätigkeitsbericht des EDÖB 2018/19*, e-paper, letzte Änderung 27.08.2019, Bern 2019, https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/26--taetigkeitsbericht-2018-20190.html.

52 Art. 10 Europaratskonvention 108 bestimmt: "Sanctions and remedies. Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

53 Kurt Pärli, in: *Stämpflis Handkommentar zum Datenschutzgesetz (DSG)* (Fn. 5), Art. 34 N 1.

54 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

55 Art. 333 Abs. 1 StGB.

beide Straftatbestände mit Busse bedroht werden, handelt es sich um Übertretungen.[56] Der Höchstbetrag der Bussen beläuft sich im geltenden Recht auf 10 000 CHF.[57]

Zusätzlich existieren weitere Straftatbestände zum Schutz persönlicher Daten im allgemeinen StGB, z.B. die Verletzung des Amts- bzw. des Berufsgeheimnisses nach Art. 320 bzw. 321 StGB, die Verletzung des Schriftgeheimnisses nach Art. 179 StGB oder das Abhören und Aufnehmen fremder Gespräche nach Art. 179bis StGB.[58]

Zivilklage

Sonstige Klagen gegen Verstösse gegen das DSG, die zu einer Persönlichkeitsverletzung führen, sind im zivilrechtlichen Verfahren geltend zu machen[59] (zum kollektiven Rechtsschutz siehe unten Frage 13).

E-DSG – Sanktionen im Datenschutzrecht de lege ferenda

Verschärfung der Strafbestimmungen

Art. 12 der Europaratskonvention 108+ verpflichtet die Vertragsparteien, bei Verletzung der Konventionsbestimmungen geeignete gerichtliche und nicht-gerichtliche Sanktionen und Rechtsmittel vorzusehen. Wie der *Explanatory Report* erläutert, hat dabei jede Vertragspartei selber festzustellen, wie sie die Massnahmen und Mittel in ihrem Land am effektivsten zivil-, verwaltungs- oder strafrechtlich ausgestaltet, wobei die gewählten Sanktionen wirksam, verhältnismässig und abschreckend sein müssen:[60]

> "It is left to each Party to determine the nature (civil, administrative, criminal) of these judicial as well as non-judicial sanctions. These sanctions have to be effective, proportionate and dissuasive. The same goes for remedies: data subjects must have the possibility to judicially challenge a decision or practice, the definition of the modalities to do so being left with the Parties. Non-judicial remedies also have to be made available to data subjects. Financial compensation for material and non-material damages where applicable, caused by the processing and collective actions could also be considered."

56 Art. 333 Abs. 3 StGB.

57 Art. 333 Abs. 3 i.V.m. Art. 106 Abs. 1 StGB.

58 Pärli (Fn. 5), Art. 34 N 1.

59 Art 28a Abs. 3 ZGB. Siehe auch EDÖB, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html#193411081.

60 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Fn. 7), N 100.

Auch nach Art. 57 der EU-Richtlinie 2016/680 wie auch nach Art. 84 Abs. 1 DSGVO müssen Sanktionen wirksam, verhältnismässig und abschreckend sein. Ein zu mildes Strafsystem im Schweizer Recht könnte zur Folge haben, dass die EU die schweizerische Regelung nicht mehr als angemessen erachtet. Vor diesem Hintergrund muss das geltende strafrechtliche Dispositiv des DSG1992 massgeblich verstärkt werden.

Die bereits im aktuellen Datenschutzgesetz bestehenden Straftatbestände werden im Rahmen der Revision z.T. übernommen und angepasst (Art. 54 ff. E-DSG):

- Weiterhin strafbar ist die Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 54 E-DSG) sowie die Verletzung der beruflichen Schweigepflicht (Art. 56 E-DSG). Letztere wird allerdings auf sämtliche geheimen Personendaten ausgeweitet.[61]
- Neu eingeführt wird ein Straftatbestand, der die Verletzung von Sorgfaltspflichten sanktioniert (Art. 55 E-DSG) und der Straftatbestand des Missachtens von Verfügungen (Art. 57 E-DSG). Dies bezieht sich auf die Tatsache, dass der EDÖB seine Verfügungen mit einer Strafandrohung versehen kann (was aber auch bedingt, dass die Verfügung hinreichend konkretisiert wird, so dass der Adressat keine Zweifel mehr über die ihm auferlegten Pflichten bzw. das vorgeschriebene Unterlassen hat).[62] In Art. 57 E-DSG wird die Bussenobergrenze von 10'000 auf 250'000 CHF erhöht, dies insbesondere mit Blick auf die Annäherung des neuen DSG an die DSGVO. Die Forderung nach noch höheren Bussen mit dem Argument, dass Unternehmen sonst zu wenig beeinträchtigt würden, hält der Bundesrat für fragwürdig. Er führt dazu aus, dass sich die Strafbestimmungen des E-DSG primär an natürliche Personen und insbesondere Leitungspersonen richten[63] (siehe auch nächste Frage).
- Mit Art. 58 E-DSG soll einerseits die Geschäftsherrenhaftung gem. Art 6 Abs. 2 des Verwaltungsstrafrechtsgesetzes (VStrR)[64] wie auch die Möglichkeit, auf die Verfolgung der strafbaren Person zu verzichten und stattdessen auf das Unternehmen zuzugreifen, eingeführt werden.
- Neben dem E-DSG soll mit Art. 179decies StGB zusätzlich ein neuer Straftatbestand ins Strafgesetzbuch aufgenommen werden, der die Verletzung der Persönlichkeit durch Identitätsmissbrauch sanktionieren soll.[65]

61 Botschaft (Fn. 19), S. 7102; Art. 35 DSG 1992 schützt demgegenüber nur „geheime, besonders schützenswerte Personendaten".

62 Botschaft (Fn. 19), S. 7103.

63 Idem, S. 7100.

64 Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (VStrR), SR 313.0.

65 Botschaft (Fn. 19), S. 7127.

Das Parlament wird diesen Strafkatalog weitgehend im Gesetz verankern[66].

Die Zuständigkeit zur Verfolgung der Straftaten bleibt wie im geltenden Recht bei den Kantonen (Art. 59 Abs. 1 E-DSG).[67] Der EDÖB kann Anzeige erstatten und die Rechte der Privatklägerschaft im Strafverfahren wahrnehmen (Art. 59 Abs. 2 E-DSG). Schliesslich soll die Verfolgungsverjährung anders als im StGB für Übertretungen vorgesehen nicht drei, sondern neu fünf Jahre betragen, dies mit der Begründung, dass Untersuchungen im Bereich Datenschutz spezifisches Wissen benötigen und aufwendig sein können.[68]

Wirksamkeit der Strafbestimmungen

Sowohl der Bundesrat wie auch das Bundesparlament gehen in der bisherigen Beratung von einer hohen Wirksamkeit des gewählten Sanktionssystems aus.[69]

In der sog. Vernehmlassung (Konsultationsverfahren im schweizerischen Gesetzgebungsprozess) wurde darauf hingewiesen, dass die Mehrheit der strafbaren Handlungen den Verantwortlichen betrifft.[70] Sofern es sich dabei um Unternehmen handelt, wird die Straftat gemäss Art 29 StGB dem Vertreter des Geschäftsorgans, also der Leitungsperson und nicht dem untergeordneten Angestellten, zugerechnet.[71] «Dies gilt insbesondere betreffend die Missachtung einer Verfügung des Beauftragten: in diesem Fall macht sich diejenige Person strafbar, die innerhalb des Unternehmens hätte dafür sorgen müssen, dass der Verfügung des Beauftragten Folge geleistet werde.»[72]

Der Verantwortlichkeit der leitenden Organe wird ebenfalls durch die Anwendbarkeit von Art. 6 VStrG Rechnung getragen:[73] Abs. 2 dieser Bestimmung sieht eine Geschäftsherrenhaftung im Unternehmenskontext vor, indem der Geschäftsherr für Taten die durch seine Angestellten begangen werden, unter Umständen einstehen muss, sofern er die Taten nicht abgewendet oder ihre Wirkungen aufgehoben hat.

Schliesslich erlaubt Art. 58 Abs. 2 E-DSG i.v.m. Art. 7 VStrR den Strafbehörden von der Verfolgung der verantwortlichen Person abzusehen und stattdessen u.U. direkt das Unternehmen zur Bezahlung der gegen die natürliche Person verhängten Busse zu verurteilen.

---

66 Vergleiche Medienmitteilung der Staatspolitische Kommission des Nationalrats, 24.1.2020: "[…] Was die Strafbarkeit betrifft in Fällen, in denen die Anforderungen an die Sicherheit personenbezogener Daten verletzt werden, hat sich die Kommission ebenfalls dem Ständerat angeschlossen. […]", https://www.parlament.ch/press-releases/Pages/mm-spk-n-2020-01-24.aspx.

67 Botschaft (Fn. 19), S. 7104.

68 Idem, S. 7104.

69 Beratung Nationalrat, 25.9.2019, Block 4, https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=47369#votum58.

70 Botschaft (Fn. 19), S. 6974.

71 Idem, S. 6974.

72 Idem, S. 6974.

73 Idem, S. 6974 f.

Späterer Systemwechsel hin zu pekuniären Verwaltungssanktionen?

Das Sanktionsregime wurde in der Vernehmlassung stark diskutiert.[74] Der Bundesrat adressiert deshalb in seiner Botschaft zum Gesetzesentwurf u.a. den durch Wirtschaftskreise unter Hinweis auf die DSGVO hervorgebrachten Kritikpunkt der fehlenden finanziellen Verwaltungssanktionen ausführlich.[75] Er führt dazu aus, dass derartige Verwaltungssanktionen in Bereiche gehören, in denen Unternehmen einer verwaltungsrechtlichen Aufsicht unterstehen, weil sie eine konzessions- oder bewilligungspflichtige Tätigkeit ausüben oder staatlich subventioniert werden.[76] Weiter weist der Bundesrat auf den strafrechtlichen Charakter solcher Verwaltungssanktionen hin, der die Einhaltung strafprozessualer Garantien verlangt, die im anwendbaren Verwaltungsverfahren indes nicht geregelt sind.[77] Die Organisation des EDÖB müsste dazu massgeblich verändert und ausgebaut werden.[78] Schliesslich soll auch nicht die bestehende Regelung der Unternehmsstrafbarkeit des Strafgesetzbuches durch die Einführung von Verwaltungssanktionen mit Strafcharakter im DSG umgangen werden.[79] Den genannten Bedenken soll umso mehr Gewicht zukommen, als der persönliche Geltungsbereich des DSG deutlich breiter als derjenige von Gesetzen mit bestehenden finanziellen Verwaltungssanktionen ist.[80] Der Bundesrat verweist daher aus Gründen der Rechtssicherheit auf die bestehende Ordnung des Verwaltungs- und Nebenstrafrechts, die zur Anwendung gelangen soll.[81] Dies hat u.a. zur Folge, dass Gewinne, die durch die Begehung der im DSG unter Strafe gestellten Taten anfallen, gem. Art. 69 ff. StGB eingezogen werden können. Dadurch kann der im Vergleich zur DSGVO eher niedrige Bussenrahmen ausgeglichen werden. Hierzu ist auch anzumerken, dass das schweizerische Strafrechtssystem generell ohne exorbitante Strafbusshöhen die sozial erwünschte individuelle Abschreckungswirkung erreicht[82], indem die begleitende Stigmatisierung durch Strafverfahren und Strafregistereintrag ungleich stärker in das Leben der Tatperson eingreifen. Eine reine summenmässige Angleichung an die Busshöhen der DSGVO ausschliesslich für den Datenschutz würde umgekehrt das soziale Verständnis zu Unrecht und Strafe überstrapazieren und kriminologisch zum konträren Effekt führen.

74 Vernehmlassungsbericht, S. 50 ff.
75 Botschaft (Fn. 19), S. 7098.
76 Idem, S. 7098.
77 Idem, S. 7098.
78 Idem, S. 7099.
79 Idem, S. 7098 f.
80 Idem, S. 7099.
81 Idem, S. 7099.
82 Vergleiche dazu die Vorgaben des schweizerischen Strafgesetzbuchs (StGB, SR 311), welches einen ganzen Tag Freiheitsstrafe mit einem monetären Wert von vergleichsweise tiefen CHF 30 - max. CHF 3 000 gleichsetzt (Art. 34 StGB i.V.m. Art. 36 StGB).

Auch die vorberatenden Parlamentskommission SPK-N (Staatspolitische Kommission des Nationalrats, also der ersten Kammer des Schweizerischen Bundesparlaments) machte sich den Systementscheid nicht leicht. Die Kommission entschied sich schliesslich nicht zuletzt im Hinblick auf die angezeigte Beschleunigung des Parlamentsverfahrens für das vorwiegend justizielle System. Zugleich aber beauftragte sie am 1.11.2018 als Nebenstrang zur Datenschutzberatung den Bundesrat, die Einführung eines allgemeinen Systems der Verwaltungssanktionen im Schweizer Recht zu prüfen, welches dann auch für das Datenschutzrecht gelten würde (wie auch etwa für das Wettbewerbsrecht, wo bereits früher eine entsprechende Sanktionsrevision versucht wurde,[83] weiter für das Fernmelderecht, den Finanzbereich etc.).[84] Der Nationalrat stimmte dem Auftrag am 4.3.2019 oppositionslos zu. Der Bundesrat wies bei dieser Gelegenheit erneut darauf hin, dass die Revision des Datenschutzgesetzes kein geeigneter Rahmen zur Klärung dieser allgemeinen und auch für andere Rechtsgebiete relevanten Grundsatzfrage sei.[85] Das Bundesamt für Justiz ist derzeit daran, den erforderlichen Bericht vorzubereiten. Je nach Ausgang könnte damit das aktuell bevorzugte justizielle Sanktionssystem in der Zukunft durch die Sanktionierung mittels finanzieller Verwaltungssanktionen wie unter der DSGVO abgelöst werden.

Frage 12

Immaterielle Schäden werden nach dem schweizerischen Haftungsverständnis grundsätzlich kompensiert. Im Datenschutzbereich verweisen sowohl das geltende Recht (Art. 15 Abs. 1 DSG 1992) wie auch Art. 28 Abs. 2 E-DSG für Klagen zum Schutz der Persönlichkeit auf die Bestimmungen über die Persönlichkeitsverletzung in Art. 28 ff. ZGB. Betreffend die Kompensation von immateriellen Schäden (Genugtuung) ist die Delikthaftungsregelung gemäss Art. 49 Obligationenrecht (OR)[86] beizuziehen. Der Genugtuungsanspruch setzt eine objektiv widerrechtliche Persönlichkeitsvoraussetzung voraus, die objektiv schwer wiegt (Bundesgerichtsentscheid BGE 117 II 50). Bei der Bemessung der Genugtuung ist wie im allgemeinen Delikthaftungsrecht die Grösse des Verschuldens wie auch die Schwere der Verletzung zu berücksichtigen.[87]

---

83 Bundesrat, Medienmitteilung, 22.2.2012: Bundesrat verabschiedet Botschaft zur Revision des Kartellgesetzes, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-43503.html.

84 18.4100 – Postulat - Instrument der pekuniären Verwaltungssanktionen, SPK-N: „Der Bundesrat wird beauftragt aufzuzeigen, wie im Schweizer Recht ein allgemeines System der pekuniären Verwaltungssanktionen sowie die erforderlichen rechtlichen Garantien eingeführt werden können."

85 Amtliches Bulletin, NR, 4.3.2019, https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=45323.

86 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches vom 30. März 1911 (Fünfter Teil: Obligationenrecht), SR 220.

87 Corrado Rampini, in: *Basler Kommentar DSG* (Fn 5), Art. 15 N 22 ff., mit Verweisungen.

Frage 13

De *lege lata* orientiert sich das seit 2008 einheitlich kodifizierte schweizerische Zivilprozessrecht[88] in Fortführung der Rechtstradition am Einzelprozess, in dem sich je eine klagende und eine beklagte Partei individuell gegenüberstehen. Sind Verhältnisse zu beurteilen, die auf gleichartigen Tatsachen oder Rechtsgründen beruhen, kommen die Bestimmungen über die sogenannte Streitgenossenschaft zum Tragen (insbesondere Art. 15 Zivilprozessordnung (ZPO)[89] betreffend die örtliche Zuständigkeit, Art. 70 ff. ZPO betreffend die Legitimation, Art. 125 lit. c ZPO betreffend die Klagenvereinigung durch das Gericht, Art. 127 ZPO betreffend die Überweisung bei zusammenhängenden Verfahren).

Mit der gesamtschweizerischen ZPO von 2008 wurde sodann aber eine Verbandsklagemöglichkeit eingeführt, gemäss der Vereine und andere Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die nach ihren Statuten zur Wahrung der Interessen bestimmter Personengruppen befugt sind, in eigenem Namen auf Verletzung der Persönlichkeit der Angehörigen dieser Personengruppen klagen können (Art. 89 ZPO). Diese Verbandsklage kann nur die Unterlassung, Beseitigung oder Feststellung einer Verletzung zum Gegenstand haben, lässt aber keine Klage auf Leistung zu. Stimmen, welche darüber hinausgehende Instrumente verlangten, blieben vorläufig ungehört.[90]

Bereits am 3.7.2013 hielt der Bundesrat aber in einem Bericht fest, dass eine Verbesserung des kollektiven Rechtsschutzes einerseits im Rahmen der bereits bestehenden Instrumente möglich wäre. Die Prozesskosten könnten beispielsweise neu geregelt, die Prozessfinanzierung gefördert und das Verbandsklagerecht erweitert werden. Andererseits wäre auch die Einführung neuer eigenständiger Instrumente der kollektiven Rechtsdurchsetzung denkbar. Namentlich könnte die Schaffung eines sogenannten Muster- oder Testverfahrens, bei welchem dem Ergebnis für gleichartige Verfahren eine verbindliche Wirkung zukäme, und unter ganz bestimmten Bedingungen möglicherweise auch eine Gruppenklage oder ein Gruppenvergleichsverfahren geprüft werden.[91] Am 27.9.2013 wurde daraufhin im Parlament eine Motion betreffend Förderung und Ausbau der Instrumente

88 Davor war die Materie kantonal und unterschiedlich geregelt.

89 Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (Zivilprozessordnung, ZPO), SR 272.

90 Vgl. etwa 13.2052 – Motion – Recht zur Sammelklage bei Datenschutzverletzungen, insbesondere im Internet, Schwab, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20133052, welche noch am 8.5.2013 vom Bundesrat negativ beurteilt wurde.

91 Bundesrat, Medienmitteilung, 2.7.2013: Kollektiver Rechtsschutz untersucht und mögliche Massnahmen aufgezeigt, https://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2013/2013-07-03/ber-br-d.pdf, mit Verweisung auf den Bericht „Kollektiver Rechtsschutz in der Schweiz – Bestandesaufnahme und Handlungsmöglichkeiten".

der kollektiven Rechtsdurchsetzung deponiert und am 13.12.2013 vom Nationalrat und am 12.6.2014 vom Ständerat angenommen.[92]

Am 17.11.2014 deponierte die Rechtskommission des Ständerats eine im Folgejahr vom Parlament angenommene Motion, gemäss welcher der Bundesrat nach einer Prüfung der Praxistauglichkeit der geltenden Zivilprozessordnung dem Parlament bis Ende 2018 erforderliche Gesetzesanpassungen zu beantragen habe].[93] Im Vordergrund stand dabei auch eine eventuelle generelle Einführung von Instrumenten des kollektiven Rechtsschutzes.

Das 2016 in Vernehmlassung gegebene E-DSG enthält vor diesem Hintergrund keine datenschutzspezifischen Bestimmungen zum kollektiven Rechtsschutz. In der Revision des DSG solle keine auf das Datenschutzrecht beschränkte Regelung der kollektiven Rechtsdurchsetzung (Erweiterung des Verbandsklagerechts und Einführung einer Sammelklage bzw. eines Sammelvergleichs) eingeführt werden. Stattdessen sollen die Instrumente der kollektiven Rechtsdurchsetzung im Rahmen der Umsetzung der erwähnten Motion in einem grösseren, möglichst sektorübergreifenden Kontext geprüft werden.[94]

Am 2.3.2018 eröffnete der Bundesrat eine Vernehmlassung über eine Revision der Zivilprozessordnung mit dem erklärten Ziel, Privaten und Unternehmen den Zugang zum Gericht zu erleichtern. Insbesondere sollen die Kostenschranken und das Prozesskostenrisiko gesenkt, der kollektive Rechtsschutz gestärkt und die Verfahrenskoordination vereinfacht werden. Mit einem Gruppenvergleichsverfahren solle eine anerkannte Lücke im Rechtssystem geschlossen und damit mehrere parlamentarische Aufträge erfüllt werden. Neu sollen Unternehmen mit einem sogenannten Gruppenvergleichsverfahren eine einvernehmliche kollektive Streiterledigung mit Wirkung für alle Geschädigten erreichen können. Weiter wurde vorgeschlagen, die Verbandsklage für die klageweise kollektive Durchsetzung von finanziellen Ansprüchen zuzulassen. Diese Massnahmen würden es Unternehmen erlauben, Ansprüche aus sogenannten Massenschäden in einem einzigen Verfahren mit einem Verbandskläger beizulegen. Dieser Ausgleich rechtswidriger Gewinne soll auch störende Wettbewerbsverzerrungen gegenüber Unternehmen beseitigen, die sich rechtskonform verhalten.[95] Die vorgesehene Anpassung und Erweiterung der Verbandsklage führe dazu, dass auch Verletzungen des Datenschutzgesetzes vermehrt und einfacher auch kollektiv durchgesetzt werden können,

92 13.3931 – Motion - Förderung und Ausbau der Instrumente der kollektiven Rechtsdurchsetzung, Birrer-Heimo, http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133931.

93 14.4008– Kommissions-Motion RK-S - Anpassung der Zivilprozessordnung, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20144008.

94 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes, a.a.O, S. 21 f.

95 Bundesrat, Medienmitteilung, 2.3.2018: Zivilprozess: Private und Unternehmen sollen leichter Zugang zum Gericht haben, https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2018/2018-03-02.html.

wie dies gerade für den Datenschutz bereits spezifisch gefordert wurde.[96] Ein definitiver Entwurf zur Ergänzung der ZPO und dessen Überweisung an das Parlament wird im Verlauf des Jahres 2020 erwartet.

Frage 14

Angesichts der Unterschiedlichkeit der Institutionen lässt sich hier keine Einschätzung abgeben.

D Datenverarbeitung für nationale Sicherheitsbelange

Frage 15

Ausgehend von der Bundesverfassung, die eine Bundeskompetenz in gewissen sensitiven Gebieten vorsieht, etwa Sicherheit, Landesverteidigung, Zivilschutz (Art. 57 ff. BV) bzw. etwas weiter entfernt Aussenwirtschaftspolitik (Art. 101 BV) ergeben sich verschiedenste Handlungsfelder, in denen regelmässig gewisse nationale Sicherheitsaspekte adressiert werden. Wie erwähnt, unterliegt die Schweiz der EU-Grundrechtecharta nicht. Mit ähnlichem Schutzbestand gilt jedoch die Europäische Menschenrechtskonvention, der die Schweiz beigetreten ist.

Eine gezielte, übergreifende Begrifflichkeit für die «nationale Sicherheit» ist zwar nicht bekannt, jedoch regeln das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)[97] und das Nachrichtendienstgesetz (NDG)[98] die relevanten Regulierungselemente betreffend die innere und äussere Sicherheit, insbesondere in Bezug auf die Informationsbeschaffung, die Datenbearbeitung durch die betreffenden Stellen und die Auskunftsrechte der Betroffenen.

Betreffend Vorratsdatenspeicherung hat das schweizerische Bundesgericht – wenn auch nicht spezifisch zur nationalen Sicherheit – im Jahr 2018 im Leitentscheid BGE 144 I 126[99] zustimmend die verwaltungsrechtliche Frage entschieden, ob die Speicherung und

96 Bundesrat, Erläuternder Bericht zur Änderung der Zivilprozessordnung (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), 2.3.2018, S. 107, https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/aenderung-zpo/vn-ber-d.pdf.

97 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21.3.1997, SR 120.

98 Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG) vom 25.9.2015, SR 121.

99 Urteil der I. öffentlich-rechtlichen Abteilung i.S. A. und Mitb. gegen Dienst Überwachung Post- und Fernmeldeverkehr sowie X. AG und Y. AG (Beschwerde in öffentlich-rechtlichen Angelegenheiten), 1C_598/2016 vom 2. März 2018 (BGE 144 I 126).

Aufbewahrung von mit dem Fernmeldeverkehr verbundenen Randdaten konform mit der Verfassung bzw. der EMRK sind:

> "Art. 15 Abs. 3 des bis zum 28. Februar 2018 geltenden Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (aBÜPF) verpflichtete die Fernmeldedienstanbieter – gleich wie das heute geltende BÜPF –, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten ihrer Kunden zu speichern und während sechs Monaten aufzubewahren (E. 3). Die Speicherung und die Aufbewahrung von Randdaten stellen einen Eingriff in die Grundrechte der Betroffenen dar, insbesondere in das Recht auf Achtung des Privatlebens, das den Anspruch auf informationelle Selbstbestimmung miteinschliesst (E. 4). Die Intensität dieses Grundrechtseingriffs ist allerdings zu relativieren: Die gespeicherten Daten betreffen nicht den Inhalt der Kommunikation und werden von den Fernmeldeunternehmen weder gesichtet noch miteinander verknüpft; für einen Zugriff der Strafverfolgungsbehörden müssen die qualifizierten gesetzlichen Voraussetzungen der Strafprozessordnung erfüllt sein (E. 5). Art. 15 Abs. 3 aBÜPF bildete für die Randdatenspeicherung eine hinreichende gesetzliche Grundlage (E. 6). Die Randdatenspeicherung und -aufbewahrung dient namentlich der Aufklärung von Straftaten; damit liegt ein gewichtiges öffentliches Interesse vor (E. 7). Die datenschutzrechtlichen Bestimmungen sehen wirksame und angemessene Garantien zum Schutz vor Missbrauch und behördlicher Willkür vor. Unter diesen Rahmenbedingungen ist auch die sechsmonatige Aufbewahrungsdauer verhältnismässig (E. 8)."

Die Beschwerde führenden Mitglieder des Vereins *digitale gesellschaft* haben den Entscheid laut Pressemitteilungen[100] wegen Verletzung von Art. 8 Ziff. 1 EMRK (Recht auf Achtung ihres Privat- und Familienlebens) an den Europäischen Gerichtshof für Menschenrechte weitergezogen. Das Strassburger Urteil steht noch aus.

100 *Computerworld*, 27.9.2018, Digitale Gesellschaft beschwert sich am EU-Gerichtshof über das Büpf, https://www.computerworld.ch/business/netzpolitik/digitale-gesellschaft-beschwert-am-eu-gerichtshof-buepf-1586693.html.

The United Kingdom

Leonard W.N. Hawkes[*]

Introduction

This report deals with the implementation of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR")[1] in the United Kingdom (UK) before the UK's exit from the EU in accordance with the European Union (Withdrawal) Act 2018 as amended. The law is stated as at 4 September 2019[2].

The main national legal instrument introduced to implement the GDPR in the UK is the Data Protection Act 2018 (hereinafter "DPA18"). The national supervisory authority's Guidance on GDPR and Brexit is available at: ico.org.uk/for-organisations/data-protection-and-brexit/.[3]

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (hereinafter "DPPExitRegs19") came into force on exit day.[4] The DPPExitRegs19 will introduce the terminology of the UK GDPR into the DPA18 and merge the existing 'applied GDPR' provisions into the UK GDPR. However, these amendments and clarifications were still to be implemented in the text of the DPA18 at this writing.[5]

---

* Solicitor of the Senior Courts of England and Wales, Member of the French speaking Order of the Brussels Bar (OBFG), established in Brussels.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [2016] OJ L119/1 (hereinafter "GDPR").

2 However, in some places it has been possible to refer to more recent developments.

3 Including 'Guidance for SMEs on how to prepare for a no-deal Brexit'. The UK Information Commissioner's Office issued a Statement on 29 January 2020, which says, amongst other things: "During [the transition] period, which runs until the end of December 2020, it will be business as usual for data protection". "The GDPR will continue to apply". (…) ICO's statement also acknowledges the potential for continuing uncertainties: "It is not yet known what the data protection landscape will look like at the end of the transition period and we recognise that businesses and organisations will have concerns about the flow of personal data in future". "We will continue to monitor the situation and update our external guidance accordingly".

4 Statutory Instrument 2019 N° 419. Exit day is defined as 31 January 2020 in the European Union (Withdrawal) Act 2018 (Exit Day) (Amendment) (No. 3) Regulations 2019, Statutory Instrument 2019 N° 1423.

5 "The applied GDPR" means the GDPR as applied by Chapter 3 of Part 2 DPA18. For processing to which it applies see DPA18 S.21. In particular Chapter 3 applies to the automated or structured processing of personal data in the course of an activity *which is outside the scope of European Union law*, DPA18 S.21(1)(a). See also DPA18 Schedule 6 on the applied GDPR.

A Setting the Scene

Question 1

The DPA18 came into force on 25 May 2018. It is a substantial piece of legislation, 349 pages long and divided into 7 Parts, with 215 Sections (hereinafter "S.") and 20 Schedules. It legislates for general data processing (Part 2); law enforcement data processing (Part 3);[6] data processing by the intelligence services (Part 4); regulatory oversight (Part 5) and enforcement and penalties for infringements (Part 6).

Part 7 contains supplementary and final provisions, including about the application of the DPA18 to the Crown and to the UK Parliament.

Part 2 of DPA18 (General Processing) applies the provisions of the GDPR to the activities of a controller or processor (as defined in the GDPR) established in the UK, and whether or not the processing takes place in the UK, (S.207 (2)).[7]

DPA18 does not contain provisions specifying processing necessary to comply with a data controller's legal obligations under A.6(1)(c) GDPR. However, S.8 DPA18 does provide a non-exhaustive list of what shall be considered processing in the 'public interest' or in the exercise of the data controller's 'official authority'.[8]

DPA18 S.9 sets the age from which a child can give consent to the processing of data for the provision of information society services at 13 years. The Information Commissioner (hereinafter "the Commissioner")[9] is under an obligation (under DPA18 S.123) to introduce an age appropriate code of practice on information society services.[10]

For processing necessary to perform or exercise obligations or rights of the controller or of the data subject under employment, social security or social protection law,[11] DPA18 introduces a requirement on the controller to put into place an "appropriate policy

6 Implementing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016], OJ L119/89 (Law Enforcement Directive, hereinafter "LED").

7 The Explanatory Notes (hereinafter "ENs") state at Note 1 ("N.1"): 'The Act also helps prepare the UK for a future outside the EU': www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf. All webpages referred to were visited 10 February 2020.

8 Art. 6(1)(e) GDPR.

9 DPA18 Ss.3(8), 114 and Schedule 12. Note however that the abbreviation 'ICO' is very often used interchangeably to refer to either the Commissioner (currently Elizabeth Denham) or the entity which she leads, the Information Commissioner's Office.

10 See now ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services.

11 Art. 88 GDPR, Processing in the context of employment.

document".[12] An appropriate policy document must (amongst other requirements) explain the controller's procedures for complying with the data protection principles.[13]

DPA18 Schedule 1 specifies the conditions and associated safeguards that must be met in order for special categories of data to be processed pursuant to DPA18 S.10. Schedule 1, Part 2, specifies conditions that must be met in order for special categories of data and personal data to be processed for reasons of substantial public interest. Schedule 1, paragraph 13 provides an additional ground for processing special categories of personal data in order to uncover dishonesty or mismanagement, provided it is in *substantial* public interest.

DPA18 Schedules 2, 3 and 4 provide restrictions and adaptations of, and exemptions from, the application of the GDPR rules.[14] Schedule 2 paragraph 4, which provides for exemptions in respect of 'effective immigration control' has been criticized.[15]

Schedule 2 Part 5 provides for the exemptions foreseen in article 85(2) GDPR for journalistic, academic, artistic and literary purposes. Derogations for scientific or historical research, statistical purposes or for archiving in the public interest (article 89 GDPR) are set out in Schedule 2 Part 6 (paras 27 and 28).

DPA18 Schedule 2, Paragraph 19, disapplies data subject information and access rights under articles 13-15 GDPR where legal professional privilege (known as 'confidentiality of communications in legal proceedings' in Scotland) can be asserted in respect of the personal data.

Question 2

As regards the Charter of Fundamental Rights of the European Union (hereinafter the "Charter") Articles 7 and 8, the situation in the UK will be affected by the eventuality of the UK's exit from the EU. A distinction needs to be drawn between a withdrawal from the EU on the basis of an arrangement implementing the revised Withdrawal Agreement[16] adopted on 19 October 2019 (an 'orderly Brexit') and an unmanaged withdrawal ('hard Brexit').

12 Schedule 1, Paragraph 1, DPA18.

13 As set-out in A5. GDPR and DPA18 S.34.

14 DPA18 S.15(1).

15 See for example Liberty's submission to the House of Commons Public Bill Committee on the Data Protection Bill, March 2018, pp. 10-25.

16 Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, 19 October 2019, https://ec.europa.eu/commission/publications/agreement-withdrawal-united-kingdom-great-britain-and-northern-ireland-european-union-and-european-atomic-energy-community_en.

What is clear is that, whether there is an orderly or a hard Brexit, the Charter will cease to apply in the United Kingdom.

In the political events surrounding the UK Parliament's failure to adopt the original Withdrawal Agreement, little attention was paid to the provisions of the European Union (Withdrawal) Act 2018 (hereinafter "EU(W)A2018"). Apart from other fundamental changes in the relationship between EU law and laws in the United Kingdom,[17] S.5(4) EU(W)A2018 excludes the Charter from retained EU law[18] even if S.5(5) goes on to state that "subsection (4) does not affect the retention in domestic law on or after exit day in accordance with this Act of any fundamental rights or principles which exist irrespective of the Charter" (…).

The Bingham Centre for the Rule of Law has commented:

> "Exactly what fundamental rights and principles are preserved (…) is not clear. The Charter itself, on the other hand, is a clear statement of articulated rights and principles. Indeed, this was the very purpose of drawing up the Charter, to provide a clear and accessible list of the rights and freedoms considered fundamental in the EU legal order".[19]

In contrast, in the EU (Legal Continuity) (Scotland) Bill, the Scottish government has expressed an intention to retain the Charter in Scots Law following EU exit. However, the retention of the Charter would only apply to devolved retained EU law.[20]

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

The Information Commissioner's Office (hereinafter "ICO") includes a discussion of fairness in its Guidance:

17 For a clear explanation of which see J. Segan, The European Union (Withdrawal) Act 2018: Ten Key Implications for UK Law and Lawyers, July 2018 at https://www.blackstonechambers.com/news/european-union-withdrawal-act-2018-ten-key-implications-uk-law-and-lawyers/.

18 "The Charter of Fundamental Rights is not part of domestic law on or after exit day".

19 For an analysis of the application of the EUCFR in the case of exemptions concerning a civil law dispute see *RFU v. Viagogo* [2012] UKSC 55 at paras 25 et seq.

20 See: The UK Withdrawal from the European Union (Legal Continuity) (Scotland) Bill -A Reference by the Attorney General and the Advocate General for Scotland (Scotland) [2018] UKSC64.

> "In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should".[21]

Three ICO decisions, (the first two decided in accordance with DPA1998), give an insight into what that general guidance means in practice:

1. True Visions Productions

TVP are a television production company. They installed cameras, with permission, in a maternity assessment unit for the purpose of filming patients for a documentary on stillbirths. TVP posted filming notices in the vicinity of the cameras and the waiting room area but did not directly and specifically inform patients that they would be filmed.

The ICO fined TVP £120,000 for failing to process patients' data fairly and lawfully. It said:

> "The processing was not fair. The patient attending (…) would not have reasonably expected there to be fixed cameras which could not be stopped in examination rooms. The patient would reasonably expect such filming expressly to be drawn to her attention. TVP did not provide sufficient fair processing information to patients, and did not sufficiently draw the information which was provided to the attention of patients", (…)[22]

2. Bounty (UK) Limited

An ICO investigation found that Bounty (UK) Limited, a pregnancy and parenting club, collected personal information for the purpose of membership registration through its website and mobile app, merchandise pack claim cards and directly from new mothers at hospital bedsides.

But the company also operated as a data broking service until 30 April 2018, supplying data to some thirty-nine third parties including credit reference and marketing agencies. The ICO fined Bounty (UK) Limited £400,000 for illegally sharing personal information belonging to more than 14 million people.

It said:

---

21 What is fairness? ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/?q=record.

22 Para. 29 of ICO's Monetary Penalty Notice ('MPN'), 8 April 2019.

> "Bounty failed to use the personal data of the affected data subjects fairly in this case. As indicated above, data subjects registering with a pregnancy and parenting club would not reasonably have expected their personal data to be disclosed to the likes of credit reference, marketing and profiling agencies".[23]

3. Her Majesty's Revenue and Customs ('HMRC') Voice ID Service

This case was an investigation made under the GDPR. It concerned the voice profiling of users of the HMRC's helplines using the words: "My voice is my password". ICO found that the voice data was collected unlawfully and issued an Enforcement Notice under DPA18 S.149 requiring HMRC to delete all of the biometric data held for which it did not have specific consent (about 5.5 million records). It said:

> "The Commissioner considers that the contravention is a significant one which warrants enforcement action. Her reasons for this conclusion include that (…) HMRC appears to have given little or no consideration to the data protection principles when rolling out the Voice ID service".[24]

Question 4

Consent

In practice, questions about obtaining informed consent have arisen most frequently in relation to direct e-mail marketing for which consent, as defined in article 4(11) GDPR is required under the e-Privacy Directive.[25] In three pre-GDPR decisions ICO found that certain customer verification requests had in fact been sent for direct marketing purposes. The ICO sanctioned such messaging in: *FlyBe, Honda* (March 2017)[26] and *BT* (June 2018)[27]. It recently confirmed this approach in *EE* (June 2019).

ICO fined EE Limited, a telecoms company, £100,000 for sending over 2.5 million direct marketing messages to its customers without consent. During the ICO investigation EE stated the texts were sent as service messages and were therefore not covered by electronic marketing rules. The ICO disagreed. It said:

23 Para. 37 of ICO's MPN of 9 April 2019.
24 Para. 24 of ICO's Enforcement Notice of 9 May 2019.
25 Directive 2002/58/EC as amended (Directive on privacy and electronic communications)
26 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/ico-warns-uk-firms-to-respect-customers-data-wishes-as-it-fines-flybe-and-honda/.
27 MPN of 20 June 2018.

> "These were marketing messages which promoted the company's products and services. The direct marketing guidance is clear: if a message that contains customer service information also includes promotional material to buy extra products for services, it is no longer a service message and electronic marketing rules apply".[28]

Legitimate interests

ICO has issued detailed Guidance on legitimate interests.[29] The Guidance includes useful practical examples:[30]

In *Bounty* (*supra* Q.3) at paragraph 39 of the MPN, ICO commented, as regards the balancing of the controller's legitimate interests against the interests or fundamental rights and freedoms of the data subjects:

> "(…) Bounty has not indicated to the Commissioner that it relies upon this condition, however the Commissioner's assessment is that this condition would not have been met (…). Given its failure to inform data subjects that their personal data may be shared with [named third-party] organisations or indeed any organisations of a similar nature, the balance of interests (…) tipped against Bounty".

As regards the benefit of conducting what it calls a Legitimate Interests Assessment (hereinafter "LIA") ICO comments:

> "An LIA is a type of light-touch risk assessment based on the specific context and circumstances of the processing. You need to record your LIA and the outcome. There is no specific requirement in the GDPR for you to do this. However, in practice you are likely to need an audit trail of your decisions and justification for processing on the basis of legitimate interests".

In light of that guidance, future decisions may show that seeking to rely on legitimate interest without having the support of an LIA report is unwise when faced with an ICO investigation.

---

28 Statement of Andy White, ICO Director of Investigations in ICO's Press Release of 24 June 2019. See also the MPN of 20 June 2019 at para. 41.

29 ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf, v1.0.20 of 22 March 2018, 46 pp. The section titled How do we apply legitimate interests in practice begins at p. 35 of the Guidance.

30 For example, regarding the issue of inter-company transfers of HR data, at p. 27 of the Guidance.

Question 5

No, there does not seem currently to be intense debate about the freedom to provide and consent to the processing of personal data in order to obtain digital content.[31] Indeed, the most serious debate on the subject seems to have been conducted within the Civil Liberties, Justice and Home Affairs Committee of the European Parliament (LIBE)[32] before the 20 May 2019 adoption of EU Directive 2019/770 on contracts for the supply of digital content and digital services.[33]

The apparent lack of debate may result from the common law's traditional *laissez-faire* attitude to the freedom to contract; it may reflect the imminence of the UK's EU exit; or as BEUC, the European consumer organisation, reported, in September 2015 (before the adoption of the digital content and digital services Directive):

> "The only country to our knowledge that has adopted a specific law for B2C contracts of digital content products is the UK.[34] This is a positive development for British consumers but at the same time it increases the risks of fragmentation across the EU if national legislators start developing their own systems to protect consumers in digital content contracts".

There is currently some speculation about whether the test for 'informed consent' will be found to be workable in practice where online direct marketing is concerned.[35]

---

31 See however, 'Why Facebook should pay us a basic income', John Thornhill, FT 7 August 2017 and Leonard Murphy, Personal Data: The Ultimate Commodity? Greenbookblog.org, 21 September 2017.

32 See: Briefing, 'Contracts for the supply of digital content and personal data protection': www.europarl.europa.eu/RegData/etudes/BRIE/2019/635601/EPRS_BRI(2019)635601_EN.pdf (PE 635.601, March 2019, and the documents cited there).

33 OJ L136/1 of 22 May 2019. EU Member States are to transpose the Directive by 21 July 2021, and it will apply from 1 January 2022.

34 The Consumer Rights Act 2015 gave consumers of digital content (software, apps, eBooks, music, videos and electronic games) new statutory rights from 1 October 2015 where purchasing digital content, or where it is supplied together with other paid for goods or services, under a contract.

35 For the ICO's recent report on AdTech see 'Update report into adtech and real time bidding", 20 June 2019 and, more recently, the 17 January 2020 blog post by Simon McDougall, ICO Executive Director of Technology and Innovation, at ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/. See also the Norwegian Data Protection Authority, Datatilsynet's, report: 'How commercial utilisation of personal data challenges privacy', November 2015, and Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt 'Third Party Tracking in the Mobile Ecosystem' 2018, in 'WebSci '18: 10th ACM Conference on Web Science, May 27–30, 2018, Amsterdam, Netherlands'.

Question 6

DPA18 S.14 provides safeguards (as foreseen by article 22(2)(b) GDPR), for significant decisions based solely on automated processing that are authorised by law. For the purposes of the section, a decision is a 'significant decision' if it either (i) produces legal effects concerning the data subject or (ii) similarly significantly affects the data subject, DPA18 S.14(2).

ICO's Guidance offers the following clarification:

> "A decision producing *a legal effect* is something that affects a person's legal status or their legal rights. For example, when a person, in view of their profile, is entitled to a particular social benefit conferred by law, such as housing benefit".
>
> "A decision that has a *similarly significant effect* is something that has an equivalent impact on an individual's circumstances, behaviour or choices. In extreme cases, it might exclude or discriminate against individuals. Decisions that might have little impact generally could have a significant effect for more vulnerable individuals, such as children."[36]

According to DPA18 S.14(4), where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing,[37]

a. the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and
b. the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to -
   i. reconsider the decision, or
   ii. take a new decision that is not based solely on automated processing.

The ICO guidance takes the pragmatic view that:

> "If you have a statutory or common law power to do something, and automated decision-making/profiling is the most appropriate way to achieve your purpose, then you may be able to justify this type of processing as authorised by law.

36 ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling-1-1.pdf. Version 05 June 2018 - 1.1.49.

37 i.e. a significant decision required or authorised by law and not necessary to a contract or made with the data subject's consent, DPA18 S.14(3).

> However, you must be able to show that it's reasonable to do so in all the circumstances".

The ICO provides the following example:

> "In the financial services sector, an organisation might use automated decision-making, including profiling, to identify fraud, in order to comply with a high level regulatory requirement to detect and prevent crime. It identifies cases of potential fraud by comparing data from credit reference agencies, bank accounts, the Land Registry, the DVLA, credit card sales, online marketplaces and social media".

Question 7

The leading authority on the right to erasure is the judgment in *NT1 & NT2 v Google*.[38] In that judgment Mr Justice Warby decided on two separate claims for erasure ('de-listing' or 'de-indexing') involving Google's Internet Search Engine ("Search"). The claims were made under the (previous) 1998 Data Protection Act (hereinafter "DPA1998"), implementing the Data Protection Directive 95/46/EC (hereinafter "DPD"). They were considered during the period when the GDPR was in force but not yet applicable.[39]

The Court took account of the decision of the Court of Justice of the European Union (hereinafter "CJEU") in *Google Spain*[40] and noted that the CJEU drew a distinction between the processing of information for journalistic purposes on the one hand, and its processing by operators of internet search engines (hereinafter "ISEs") on the other, suggesting that the rights of data subjects will vary accordingly.

The Court qualified the right to erasure (by reference to its description as a right to be forgotten) in the following way:

> "… it may be misleading to label the right asserted by these claimants as the "right to be forgotten". They are not asking to "be forgotten". The first aspect of their claims asserts a right not to be remembered inaccurately. Otherwise, they are asking for accurate information about them to be "forgotten" in the

38 Judgment of 13 April 2018, *NT1 & NT2 v Google* [2018] EWHC 799.

39 A summary and a copy of the judgment are available at: www.judiciary.uk/judgments/nt1-nt2-v-google-llc-right-to-be-forgotten/. Para. 13 of the Judgment helpfully summarises the existing legal framework, taking the enactments and the corresponding common law developments in chronological order.

40 Judgment of 13 May 2014 in Case C-131/12 *Google Spain SL & another v Agencia Espanola de Proteccion de Datos (AEPD) and another* [2014] ECLI:EU:C:2014:317.

> narrow sense of *being removed from the search results returned by an ISE in response to a search on the claimant's name*. No doubt a successful claim against Google would be applied to and by other ISEs. But it does not follow that the information at issue would have to be removed from the public record … And a *successful delisting request* or order in respect of a specified URL will not prevent Google returning search results containing that URL; it *only means that the URL must not be returned in response to a search on the claimant's name*. [para. 38] (Emphasis added.)

The ICO issued up-dated guidance on the right to erasure on 22 May 2019.[41] DPA18 requires the Commissioner to produce a code of practice that provides practical guidance and promotes good practice regarding processing personal data for the purposes of journalism. ICO's consultation on this code of practice was closed on 24 May 2019.[42] In the meantime, ICO's current (2014) guidance 'Data protection and journalism: a guide for the media' remains available.[43]

Question 8

Regarding processing and freedom of expression and information, the measures notified by the United Kingdom[44] were Ss.15, 143, 147, 152 and 174-179, and paragraph 26 of Schedule 2 and Schedule 17 to the DPA 2018.[45] In Schedule 2, Part 5 contains exemptions or derogations from Chapters II, III, IV, V and VII of the GDPR for reasons relating to freedom of expression, as permitted by article 85(2) GDPR.[46]

A court must *stay* (or, in Scotland, *sist*) special purpose proceedings, pending a decision of the Commissioner or withdrawal of the claim, if the controller or processor claims, or it appears to the court, that any personal data to which the proceedings relate is: a) only being processed for the special purposes, b) is being processed with a view to the publication of journalistic, academic, artistic or literary material, and c) has not previously been published by the controller, DPA18 S.176(1).

41 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/.

42 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-a-data-protection-and-journalism-code-of-practice/.

43 https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

44 In accordance with art. 85(3) GDPR.

45 GDPR: notification letter of 24 May 2018 to Martin Selmayr, Secretary General European Commission, from UK Permanent Representation, available from: https://ec.europa.eu/info/sites/info/files/uk_notification_51.4_84.2_85.3_publish.pdf.

46 DPA18 S.15(1).

The provisions of DPA18 S.176(1) are substantially the same as those of article 32(4) DPA1998 (implementing the DPD) which were the subject of the Court of Appeal's judgment in the *Stunt* Case.[47] In that case the Appellant (*Stunt*), appealed a High Court Order granting Associated Newspapers Limited (*Associated*) a stay of proceedings under DPA1998 S.32(4) on the basis that the personal data it held was being processed for journalistic purposes with a view to publication.

The Court of Appeal's judgment in the *Stunt* Case has led to a reference to the CJEU, on whether provisions such as S.32(4) DPA1998 are compatible with the requirements of DPA1998 S.9 that an exemption for journalistic purposes, or artistic or literary expression, should only be permitted to the extent that it balances the right to privacy (and protection of personal data) with freedom of expression and with articles 7, 8 and 47 of the Charter.[48]

If the reference is ever heard, it should help to clarify what margin of discretion a state has to adopt measures (such as DPA1998 S.32(4) and DPA18 S.176(1)) intended to prevent the chilling effect on free speech exemptions of applications to enforce data protection rights and the individual's right to protection of personal data and a remedy for failure to respect that right.[49]

C Domestic Enforcement of Data Protection Law

Question 9

The ICO is the information rights regulator for the UK. It describes its mission as 'Upholding information rights for the UK public in the digital age'. Amongst its strategic goals it lists:

- Increase the public's trust and confidence in how data is used and made available;
- Improve standards of information rights practice through clear, inspiring and targeted engagement and influence;
- Enforce the laws it helps shape and oversee.[50]

47 *James Stunt v Associated Newspapers Limited* [2018] EWCA Civ 1780.

48 Notice of Application, *SY v Associated Newspapers Ltd.*, published in OJ *C* 25 of 21.01.2019, at p. 27.

49 In Mosely, *Mosely v United Kingdom* [2012] EMLR 1 the European Court of Human Rights (hereinafter "ECtHR") found that the UK was not in breach of its obligations under Article 8 of the European Convention on Human Rights (hereinafter "ECHR") by failing to impose a duty on the News of the World to notify the applicant in advance of publication of material which violated respect for his private life – thereby denying him the opportunity to apply for an interim injunction to prevent such publication. See the ECtHR's judgment at para. 122 and the discussion of Mosely at paras 88-91 and 98 of the judgment of the majority in the *Stunt* Case.

50 ICO Annual Report 2018/19 at p. 11 - mission, vision, strategic goals and values.

The Commissioner is a corporation sole.[51] The Commissioner must appoint one or more deputy Commissioners and may appoint other officers and staff on merit on the basis of fair and open competition. The Commissioner has responsibility for determining the remuneration and conditions of service of her officers and staff.[52]

The legislation that the ICO-regulates is not only the DPA18 and GDPR, but also the:

- Freedom of Information Act 2000 (FOIA);[53]
- Environmental Information Regulations 2004 (EIR);
- Privacy and Electronic Communications Regulations 2003 (PECR);
- Network and Information Systems Regulations 2018 (NIS);
- infrastructure for Spatial Information in the European Community Regulations 2009 (INSPIRE);
- Reuse of Public Sector Information Regulations 2015 (RPSI);
- Investigatory Powers Act 2016 (IPA);
- Electronic Identification and Trust Services for Electronic Regulations 2016 (eIDAS).

The Commissioner's annual report and financial statements 2018-2019 concerns the twelve months ending on March 2019.[54] The report is divided into three major sections (A, B and C). Part A deals with the implementation of the DPA 2018 and the GDPR.

The 'Action we have taken' drop-down tab on the ICO's website[55] shows that between 25 May 2018 and 4 September 2019 ICO took 68 enforcement actions in total. It issued 38 Monetary Penalty Notices, 18 Enforcement Notices, brought 11 Prosecutions and took Undertakings in one case.

In addition to the statutory codes provided for in the DPA18 (on age-appropriate design, data sharing, direct marketing and data protection and journalism[56]), ICO is developing guidance for the use of personal data in political campaigns. This work emerged

51 A public office created by an act of Parliament occupied by a (single) natural person. The appointment is made by the Crown. DPA18 Schedule 12, paras 1 and 2.

52 DPA18 Schedule 12, para. 5.

53 Regarding processing and public access to official documents (GDPR A86), the Freedom of Information Act 2000 (FOIA) covers any recorded information held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. (Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.) The FOIA does not give people access to their own personal data (health records or credit record for example).

54 Published on 8 July 2019: ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

55 ico.org.uk/action-weve-taken/.

56 As required by respectively S.121, S.122, S.123 and S.124 DPA18.

from its Democracy Disrupted policy report[57] published in July 2018 following its investigation into the use of personal data in data analytics campaigns by political parties.[58]

Question 10

The ICO homepage provides two possibilities for making a complaint.[59] There is a drop-down tab at the top of the opening page entitled 'Make a Complaint' and there is a 'Take Action' column on the right of the opening page which has three headings one of which is 'Make a Complaint'.

The Commissioner's 2018-2019 annual report[60] refers to an 'unprecedented year'. It notes that ICO's workforce grew from 505 to more than 700 over that period, "with particular increases in the parts of the organisation handling data protection complaints and customer contact".

ICO states that its approach to its enforcement responsibilities is intelligence led.

> "To make sure that our investigation and enforcement work is targeted in the right areas, we developed an Intelligence Strategy to set out how we use the information we gather. One important piece of work in this area is using the information we receive from the public and other sources to inform a strategic threat assessment, which will support all of our work, including investigations, enforcement, guidance, codes of practice and more". (…). [p. 28]

ICO also notes that its enforcement powers have increased:

> "Under the GDPR and DPA 2018, we are able to issue formal assessment notices to any organisation, either public or private. Under the DPA 1998 the Commissioner only had compulsory audit powers in respect of central government and health organisations". (…) With these new powers of inspection, we have been able to proactively respond to complaints from the public about unsolicited marketing communications and unfair and unlawful processing". [p. 23]

57 Available at: ico.org.uk/media/2259369/democracy-disrupted-110718.pdf.

58 Specific findings in relation to the harvesting of Facebook data, Cambridge Analytica and Global Science Research, are included in a separate investigation report at: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

59 https://ico.org.uk/.

60 Op cit.

A concrete example concerned the use of mobile phone extraction for policing [p. 26].

2018-19 saw a significant increase in the number of data protection complaints reported to ICO by the public. During 2018-19, it received 41,661 data protection complaints from the public compared with 21,019 complaints received in 2017-18. ICO closed 34,684 complaints in 2018-19, compared to 21,364 in 2017-18, but it carried forward a caseload of 9,503 data protection complaints into the new reporting year.

In order to maintain service standards for the public, ICO wants to reduce open complaints across 2019-20 to below 5,000. In terms of the types of complaints received, subject access requests (SARs) were the most frequent complaint category, representing 38% of data protection complaints received. (This was similar to the proportion before the GDPR and DPA 2018 (39%). [pp. 30-32].

Question 11

ICO laid its Regulatory Action Policy (hereinafter "RAP") before Parliament in July 2018 and received approval in November 2018. The objectives set out in the RAP [pp. 22-23], include to:

– Be effective, proportionate, dissuasive and consistent in application of sanctions, targeting the most significant powers on organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data.

Enforcement notices compel a data controller to comply with data protection laws within a specified time. In an investigation relating to Her Majesty's Revenue and Customs (HMRC) and its Voice ID service for customer identification ICO found that HMRC had failed to give customers sufficient information about how their biometric data would be processed and failed to give them the chance to give or withhold consent.[61] The enforcement notice required HMRC to delete all biometric data held under the Voice ID service for which they did not have explicit consent. [p. 24].

As part of ICO's investigation into the use of personal data in political campaigns (launched under the DPA 1998), it requested a search warrant, which meant a 17-day delay to gain access to Cambridge Analytica's premises. Under GDPR and DPA 2018, ICO's powers have broadened and 'assessment notices', mean that ICO is now able to gain access

61 Another enforcement notice concerned the Metropolitan Police Service's (MPS) 'Gangs matrix', see further: ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf.

to a company's premises and data protection practices much faster than under the previous legislation.[62]

Outside the period covered by its annual report, ICO issued two notices of intention to fine under GDPR and DPA 2018 against British Airways (£183.39 million)[63] and Marriott International (£99,200,396)[64] respectively. In both cases ICO investigated as the lead supervisory authority on behalf of other EU Member State data protection authorities, who may comment on the ICO's findings under the GDPR 'one stop shop' provisions. Neither fine had been confirmed at the time of writing.

Under the Public Interest Disclosure Act 1998, the ICO is a 'prescribed person' which means that whistleblowers are provided with protection when disclosing certain information. 319 whistleblowing disclosures were made to ICO during the period 1 April 2018 to 31 March 2019. Further action was taken on 135 of the disclosures and of those 135 disclosures:

- 55 disclosures were taken into consideration for ongoing investigations;
- 28 disclosures were considered as data protection complaints.[65]

Question 12

S.168 DPA18 implements the right to claim damages set out in article 82 GDPR. The fact that article 82 GDPR makes explicit that data subject should be compensated for damages suffered for both tangible and intangible (material and non-material) harm is to be welcomed.

Under the previous legislation, the scope of the right to compensation for damage under S.13 DPA1998, implementing article 23 of the Directive 95/46/EC (DPD), was considered by the English Court of Appeal in the important *Vidal-Hall* case.[66]

The claimants in *Vidal-Hall* used the Safari browser on Apple computers to access the internet. Contrary to what they had been informed, browser generated information (hereinafter "BGI") was collected by the defendant, to track their internet usage, without their knowledge or permission, and the BGI was used by advertisers to send them targeted advertising [paras 2 and 3].[67] A fundamental issue in the case was the scope of the right to

62 Normally after 7 days, but it may be less (DPA18 S.146 (8) and (9).

63 ICO Statement in response to an announcement to the London Stock Exchange that the ICO intends to fine British Airways for breaches of data protection law, 8 July 2019.

64 Statement in response to Marriott International, Inc's filing with the US Securities and Exchange Commission that the ICO intends to fine it for breaches of data protection law.

65 See further ICO Annual Report 2018/2019 (op cit), Part A, Performance report: Whistleblowing disclosures at p. 71.

66 *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311 (ICO intervening).

67 On the subject of adtech and real time bidding see the ICO's up-date report: ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf of 20 June 2019.

'damages' in DPA1998 S.13, including whether there could be a claim for compensation without pecuniary loss.

The meaning of 'damage' in section 13 of the DPA1998

In the second part of the judgment [paras 52-105] the court considered the problem caused by the express limitation on the right to claim [non-tangible] damages introduced by DPA1998 S.13(2). Whereas S.23 DPD provided (generally) that Member States should provide that any person who suffered damage as a result of unlawful processing was entitled to compensation from the controller: the DPA1998 S.13(2) limited the right for damages for distress to cases where (a) there was also direct damage (under S.13(1)); or (b) where the processing related to journalism, artistic or literary purposes (the 'special purposes')). Neither (a) nor (b) applied to any of the *Vidal-Hall* claimants [para. 83].

The Court found [para. 76] that article 23 of the DPD must be given its natural and wide meaning so as to include both material and non-material damage. However, it found that the principles in the *Benkharbouche* Case, permitted it to disapply S.13(2).[68] Further, it found, relying on article 47 of the Charter, that it could disapply S.13(2) DPA1998 without needing to devise a substituted scheme (which would have been Parliament's prerogative).

> "As this court stated in Benkharbouche (…), (iv) in so far as a provision of national law conflicts with the requirement for an effective remedy in article 47, the domestic courts can and must disapply the conflicting provision; and (v) the only exception to (iv) is that the court may be required to apply a conflicting domestic provision where the court would otherwise have to redesign the fabric of the legislative scheme". [para. 105]

Although the Court of Appeal refused permission, the Supreme Court granted leave for the *Vidal-Hall* judgment to be appealed on one point, but, on 30th June 2016, Google withdrew its appeal after the parties reached a settlement.

Question 13

The area of the collective representation of claimants is undergoing important developments in England and Wales. Aside from the specific statutory provisions in the former DPA1998 and now in DPA18, and the courts' general powers of case management,[69] Part 19 of the Civil Procedure Rules (hereinafter "CPR") in England and Wales foresees two main forms

68 *Benkharbouche and Janah v Embassy of Sudan and others* [2015] EWCA Civ 33 at paras 69 to 85.
69 CPR Part 3 CPR.

of collective action. They are the Group Litigation Orders (hereinafter "GLO")[70] and Representative actions (hereinafter "RA").[71,72]

Where there are a number of claims that give rise to common or related issues of fact or law ('GLO issues') the court may make a GLO.[73] Where more than one person has the same interest in a claim, the claim may be begun as a *representative* of any other persons who have that interest (RA).[74]

S.187(1) DPA18 concerns the ability of representative bodies to exercise relevant rights on behalf of data subjects, provided that they are authorized to do so by the data subjects (opt-in). In relation to the GDPR the relevant rights[75] include the right to apply for a court order against, and the right to receive compensation from a controller or processor.[76] What qualifies as a representative body is defined in S.187(3) and (4).[77]

What is unclear is whether S.187(3) and (4) also need to be read subject to S.168(2)(a) DPA18[78] which apparently (indirectly) imposes the additional requirement that proceedings for compensation must be brought by a representative body within the meaning of the CPR. If that is right, as noted above, the claimants must all have the 'same interest'. That, may result in a restriction on the ability to bring such representative actions, as what constitutes the 'same interest' has been narrowly defined by the courts[79] as identity of interest.[80]

A GLO is seemingly in course of preparation in respect of the BA Data Breach,[81] where ICO's final decision is under consideration.[82] However, no such GLO had been listed as at 31 August 2019.[83] The court's decision not to permit a representative action in respect of the so-called 'Safari workaround' in *Richard Lloyd v Google LLC* [2018] EWHC 2599,

70 CPR Part 19 section III CPR.

71 CPR Part 19 section II Rule 19.6 Representative parties with same interest.

72 These are all 'opt-in' procedures. The opt-out procedure is not currently implemented by DPA18. Note that the Civil Litigation (Expenses and Group Proceedings) (Scotland) Act 2018 will permit both opt-in and opt-out procedures before the Scottish Courts once rules of court have been introduced to give it effect.

73 CPR Rule 19.11.

74 See further CPR Rules 19.6 (1) and 19.6 (4).

75 As defined in art. 80(1) GDPR.

76 As provided by art. 82(1) GDPR.

77 By reference to the art. 80(1) GDPR criteria.

78 Payment of compensation to a representative body may be made where proceedings under art. 82 of the GDPR - "are brought in accordance with rules of court" - by a representative body.

79 For a helpful review of the case law see the judgment of the Lord Chancellor in *Emerald Supplies Ltd. v British Airways plc* [2009] EWHC 741, at paras 10-24.

80 The Emerald Supplies judgment was subsequently approved by the Court of Appeal [2010] EWCA Civ 1284, which examined the scope of CPR 19.6. See per Mummery LJ at paras 62-65.

81 See www.badatabreach.com/.

82 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

83 www.gov.uk/guidance/group-litigation-orders#list-of-all-group-litigation-orders.

was the subject of an appeal which was heard in mid-July 2019.[84] The Court of Appeal subsequently overturned Warby J's judgment and granted Mr Lloyd permission to serve a representative action on Google out of the jurisdiction.[85]

The *Morrisons* Case,[86] which concerns the ('vicarious') liability of the employer for deliberate disclosure of employees payroll data, is the subject of an appeal to the Supreme Court which was heard on 6-7 November 2019.[87]

Question 14

The ICO is a unitary regulator of information rights in the UK with a variety of responsibilities outside the application of the GDPR. The relevant ICO webpage refers to memorandums of understanding (hereinafter "MOU") and other documents which outline the responsibilities and agreements held between the ICO and other authorities.[88] At this writing the page and underlying documents were being updated to ensure that the MOUs (with almost thirty regulators or ombudspersons) are compliant with GDPR and DPA18 requirements.

D Data Processing for National Security Purposes

Question 15

Part 3 of the DPA18 implements the Law Enforcement Directive (hereinafter "LED").[89] As a separate section of its Guide to Data Protection, ICO has published a Guide to Law Enforcement Processing.[90] DPA18 Part 3 only applies to processing for law enforcement purposes by the competent authorities,[91] processing which they carry out which is not for the primary purpose of law enforcement will be covered by DPA18 Part 2.[92]

84 *Richard Lloyd v Google* LLC [2018] EWHC 2599. See www.youoweus.co.uk/google-owe-us-court-appeal-today/.

85 *Richard Lloyd v Google* LLC [2019] EWCA Civ 1599.

86 *WM Morrisons Supermarkets plc v Various Claimants* [2018] EWCA Civ 2339.

87 The UK Supreme Court, WM Morrisons Supermarkets plc (Appellant) v Various Claimants (Respondent), Case ID: UKSC 2018/0213. Appeal allowed 1 April 2020 [2020] UKSC 12.

88 https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/.

89 Directive (EU) 2016/680, [2016], OJ L119/89.

90 25 April 2019 [version] 1.1.7. See also, for example, www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/.

91 The list of competent authorities in Schedule 7 DPA18 covers the principal police and other criminal justice agencies in the UK which are subject to the provisions of this Part but see also S.30(1)b.

92 As regards the use of Automated Facial Recognition technology by the police see the judgment of 4 September 2019 in *Bridges v Chief Constable of South Wales* [2019] EWHC 2341, in which the Court

The processing of personal data controlled by an intelligence service (the Security Service, Secret Intelligence Service and Government Communications Headquarters) is governed by Part 4 of the DPA18.

Broadly speaking, the provisions of Part 4 of DPA18 accord respect for the fair processing principles of the GDPR[93] and the rights of data subjects.[94] However, Section 110 creates an exemption from provisions of Part 4 (as well provisions in Part 5 and Part 6) if that exemption is required for the purpose of safeguarding national security.

Under DPA18 S.79 a Minister of the Crown may certify that a restriction on data subject rights is necessary and proportionate to protect national security.[95] The Commissioner is required to publish information about the existence of national security certificates.[96]

The Charter will cease to be part of UK law as from the EU Exit Date. Even if the Court of Appeal in its influential *Vidal-Hall* judgment expressly relied on article 47 of the Charter in respect of the right to a remedy: the courts would seemingly not be able to apply reasoning based on the Charter in any future case where similar issues arose.[97] They might base similar reasoning on the UK's Human Rights Act 1998 and the European Convention on Human Rights (ECHR) but regarding the balance between international human convention rights and UK statute law, there may in future be less room for such judicial interpretation.[98]

---

found that the South Wales Police's use of its AFR Locate technology was consistent with the requirements of the Human Rights Act 1998 and the data protection legislation. See also the report: 'ICO investigation into how the police use facial recognition technology in public places' of 31 October 2019 (available at ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf and the Information Commissioner's Opinion: 'The use of live facial recognition technology by law enforcement in public places', also of 31 October 2019 (available at ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

93 Ss. 85-91 DPA18.

94 Ss. 92-100 DPA18.

95 For the purposes of Ss. 44(4), 45(4), 48(3) and 68(7) DPA18.

96 The exemptions in respect of national security are provided for at DPA18 Ss.26 and 110 and in DPA18 Part 3. A list and certain details of the certificates are available at: ico.org.uk/about-the-ico/our-information/national-security-certificates/.

97 See also the DPPExitRegs19, (op cit, note 4), and Regulation 5 in particular which clarifies, amongst other things, that 'retained case law' and 'retained general principles of EU law' have the same meaning as in the European Union (Withdrawal) Act 2018 (see section 6(7) of that Act).

98 See further on this point, Lord Sumption in The BBC Reith lectures 2019: Law and the decline of politics. Lecture 3: *Human rights and wrongs* at p. 5, 7 and 8 of the lecture transcript.

List of FIDE 2020 Partners

List of FIDE 2020 Partners

Institutional Partners/Partenaires institutionels/Institutionelle Unterstützer

Court of Justice of the European Union

European Commission

Ministerie van Buitenlandse Zaken

Den Haag

Universiteit Leiden

Autoriteit Consument & Markt

Universiteit Leiden Europa Institute

Raad van State

de Rechtspraak

Ministerie van Economische Zaken en Klimaat

de Rechtspraak College van Beroep voor het bedrijfsleven

Sponsors/sponsors/Sponsoren

Allen & Overy

Boom juridisch

eleven international publishing

Brinkhof

De Brauw Blackstone Westbroek

Defares

大成 Dentons

Freshfields Bruckhaus Deringer

Houthoff

Loyens & Loeff

Pels Rijcken

Stibbe

Media Partner

EU Law Live

stay alert | keep smart