EU privacy and data protection law applied to AI: unveiling the legal problems for individuals

Häuselmann, A.N.

3 The current legal framework

This chapter aims to answer the second research question, namely, what the current EU legal framework is. First, Section 3.1 of this chapter describes the current legal framework regarding the fundamental right to privacy followed by Section 3.2 which introduces the fundamental right to data protection. Next, Section 3.3 discusses the most relevant piece of EU secondary law in data protection, namely, the GDPR. Finally, the ePrivacy Directive will be introduced (Section 3.4). Section 3.5 answers Subquestion 2.

As indicated in Sections 1.1 and 1.4, and as apparent from Chapters 4 and 5, I focus on horizontal relationships and EU secondary law. This focus is also visible from the corresponding sub-sections of this chapter. The introduction of the fundamental right to data protection according to Article 8 EUCFR is brief. Nonetheless, Article 8 EUCFR is relevant because the GDPR aims to ensure a high level of protection 'of the rights guaranteed in Article 16 TFEU and *Article 8 of the Charter*'.[290] The GDPR 'implements'[291] this fundamental right and covers horizontal relationships. The principle of proportionality discussed in Section 3.2.2 is a general principle of EU law. It is relevant not only in the context of Article 8 of EUCFR but also when interpreting the GDPR.

The distinction between the fundamental right to privacy (Article 7 EUCFR) and data protection (Article 8 EUCFR) is not purely symbolic. Case law of the European Court of Justice (CJEU) shows that despite substantial overlaps, there are differences with the scope of both rights and their limitation.[292] Imagine, for example, a smart advertisement board in a supermarket powered by software that deploys computer vision and affective computing approaches to analyse the faces of customers that look at the ad board to determine their emotional states, age and sex without the possibility to identify them. Such a scenario would trigger the scope of application of the fundamental right to privacy,[293] but arguably not the right to data protection because individuals cannot be identified.[294] Nevertheless, privacy law is often used as a synonym for data protection law. Admittedly, the distinction is very semantic, similar to a debate on whether a hot dog can also be considered a sandwich.

[290] Case C-645/19 [2021] *Facebook Ireland* ECR I-483 para 45 emphasis added by the author; see also Case C-319/20, *Meta Platforms Ireland Limited* [2022] ECR I-322 para 73.
[291] Article 1 (2) GDPR which reveals the main objective of said regulation: to give meaning to this fundamental right see Hielke Hijmans, Commentary of Article 1 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 56.
[292] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222.
[293] See Section 3.1.
[294] No personal data are processed; see Section 3.3.1 below.

3.1 The fundamental right to privacy

The human right to respect for private and family life as enshrined in Article 8 of the Council of Europe's European Convention for Human Rights (ECHR) and the corresponding fundamental right according to Article 7 of the EU Charter of Fundamental Rights (EUCFR) protect everyone's 'right to respect for his private and family life, his home and correspondence'.[295] Because the European Court of Justice (CJEU) held that Article 8 ECHR and Article 7 EUCFR must be interpreted *identically*,[296] I refrain from assessing the scope and meaning of these rights separately. Therefore, the following analysis applies to both rights equally. I deliberately focus on the case law of the European Court of Human Rights (ECtHR) because it is more developed than CJEU case law.[297] Within this thesis, I use the term 'private and family life' and 'privacy' interchangeably. As the attentive reader already noted, the EUCFR considers privacy to be a 'fundamental right' and the ECHR to be a 'human right'. The former is commonly used to allude to rights that are granted a special status by a certain legal order, and the latter to rights recognised in international law.[298] Because this thesis focusses on EU law, I use the term 'fundamental right'.

3.1.1 Scope

The essential object of Article 8 ECHR is to protect an individual against 'arbitrary interference by the public authorities' with its private and family life, home and correspondence.[299] This obligation is of the classic negative kind, but the ECtHR emphasised[300] that Article 8 ECHR also entails a positive obligation which requires the state to take steps to provide particular rights or to protect people against the activities of other private individuals.[301] In a Resolution, the Council of Europe stated that the right to privacy granted under Article 8 ECHR 'consists essentially in the right to live one's own life with a minimum of interference'.[302] The ECtHR cited this Resolution in its jurisprudence, including cases where non-state actors infringed the right to privacy.[303] The text in Article 8 (1) ECHR demands for respect of private and family life, home and correspondence. What the term 'respect' means is, even in the view of the ECtHR, not 'clear-cut', in particular 'where the positive obligations implicit in that concept are concerned'.[304] What seems relevant here is one of the fundamental principles in a

[295] Note that the wording of Article 7 EUCFR includes 'communications' instead of 'correspondence' as in Article 8 ECHR. However, the two terms essentially mean the same.
[296] Case C-400/10, *J. McB.* [2010] ECR I-582 para 53; Case C-450/60, *Varec SA* [2008] ECR I-91 para 48.
[297] Frederik Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting' (Doctoral thesis, Universiteit van Amsterdam 2015) 99 <https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5> accessed 8 February 2024.
[298] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 164, 166.
[299] *Niemietz v Germany* App no 13710/88 (ECtHR, 16 December 1992) para 31.
[300] *Marckx v Belgium* App no 6833/74 (ECtHR, 13 June 1979).
[301] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 502.
[302] Council of Europe, 'Resolution 428 Declaration on mass communication and Human Rights' (1970) para 16.
[303] *Von Hannover v Germany (No. 1)* App no 59320/00 (ECtHR 24 September 2004) para 42; *Von Hannover v Germany (No. 2)* App no 40660/08 and 60641/08 (ECtHR 07 February 2012) para 71; *Mosley v United Kingdom* App no 48009/08 (ECtHR 10 May 2011) para 56.
[304] *Mosley v United Kingdom* App no 48009/08 (ECtHR 10 May 2011) para 108.

democratic society, namely, the rule of law, which dictates the existence of measures of legal protection against arbitrary interference by public authorities with the rights protected by the ECHR.[305]

The following sections elaborate on the protected elements of the fundamental right to privacy that are specifically relevant in the context of this research. These two elements are private life (Section 3.1.1.1) and communication (Section 3.1.1.2).[306] Subsequently, the living instrument doctrine (Section 3.1.2) applied by the ECtHR will be introduced.

3.1.1.1 Private life

The notion of private life is considered to be a broad concept that includes the ability to live one's own life without arbitrary disruption or interference.[307] Thus, the most traditional aspect of the right to private life is the individual's interest in not being exposed to unwanted attention from the state or third parties.[308] In its case law, the ECtHR consistently emphasised that the concept of private life is incapable of an exhaustive definition.[309] However, the case law provides insight into the rather wide range of rights and interests covered under the notion of private life.[310] The interpretation of the term 'private life' in Article 8 is 'underpinned by the notions of personal autonomy and quality of life'.[311] Therefore, the term 'private life' is not limited to an 'inner circle' but encompasses the sphere of personal autonomy within which everyone can freely pursue the development and fulfilment of their personality and establish and develop relationships with other people and the outside world.[312] The right to respect for private life entitles the individual concerned to control the use of its image, including the right to object to the publication of a photograph and to the recording, conservation and reproduction of the image by another person.[313] An individual's image constitutes an essential attribute of personality because 'it reveals the person's unique characteristics and distinguishes the person from his or her peers.'[314] Also, secret surveillance invades an individual's private space[315] and thus interferes with the right to respect private life and correspondence.[316] A violation of the right to respect for private life may even occur when the information obtained by means of secret surveillance measures

[305] *Södermann v Sweden* App no 5786/08 (ECtHR 12 November 2013) para 75; *Tavi v Turkey* App no 11449/02 (ECtHR 9 November 2006) para 28; *Ciubotaru v Moldova* App no 27138/04 (ECtHR 27 April 2010) para 50; David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 368.
[306] In Sections 5.2-5.5, four specific dimensions covered by these two main elements will be discussed in more detail.
[307] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 503, 504.
[308] Karin de Vries, 'Right to Respect for Private and Family Life' in Pieter van Dijk et al (eds) *Theory and Practice of the European Convention on Human Rights* (Intersentia 2018) 670.
[309] *Niemietz v Germany* App no 13710/88 (ECtHR, 16 December 1992) para 29; *Pretty v United Kingdom* App no 2346/02 (ECtHR 29 April 2002) para 61; *Peck v United Kingdom* App no 44647/98 (ECtHR 28 January 2003) para 57.
[310] Karin de Vries, 'Right to Respect for Private and Family Life' in Pieter van Dijk et al (eds) *Theory and Practice of the European Convention on Human Rights* (Intersentia 2018) 670.
[311] *Pretty v United Kingdom* App no 2346/02 (ECtHR 29 April 2002) paras 61and 62: Christine Goodwin v United Kingdom App no 28957/95 (ECtHR 11 July 2002) para 90.
[312] William Schabas, *The European Convention on Human Rights: A Commentary* (OUP 2015) 369.
[313] William Schabas, *The European Convention on Human Rights: A Commentary* (OUP 2015) 377.
[314] *Reklos and Davourlis v Greece* App no 1234/05 (ECtHR 15 January 2009) para 40.
[315] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 533.
[316] Karin de Vries, 'Right to Respect for Private and Family Life' in Pieter van Dijk et al (eds) *Theory and Practice of the European Convention on Human Rights* (Intersentia 2018) 670.

is not used subsequently.[317] Thus, it is the surveillance itself that counts as an interference with an individual's privacy.[318]

Three particular dimensions of privacy derived from the element 'private life' will be further discussed in Chapter 5, namely, when they are applied to AI. These are informational privacy (Section 5.2), bodily privacy (Section 5.3) and mental privacy (Section 5.4).

3.1.1.2 Communications

Compared to Article 8 ECHR, the wording of Article 7 EUCFR includes 'communications' instead of 'correspondence'. In essence, the two terms mean the same thing. Both mail and electronic messages fall within the scope of 'correspondence' and under 'communication'. The same applies to telephone calls and similar forms of communication[319] relying on the Internet, such as messenger apps. In other words, the right to respect correspondence protects private communications regardless of their form or content. The term 'correspondence' has been interpreted by the ECtHR in a manner that allows one to keep up with technological developments. It covers telephone, facsimile, email, Internet usage, letters and, most importantly, also other methods of communication in the future.[320] Furthermore, Article 8 of the ECHR protects both private and business-related correspondence, regardless of whether it is carried out from an office or from a private home.[321]

3.1.2 Living instrument doctrine

Article 8 requires the ECtHR to determine issues at the forefront of technology or issues that concern sensitive societal views and values. In this regard, the broad principles of Article 8 have allowed the ECtHR to continuously respond to modern legal dilemmas and human rights challenges.[322] The ECtHR has refused to define the ambit of Article 8 ECHR[323] and 'does not consider it possible or necessary to attempt an exhaustive definition of the notion of private life',[324] which allows the ECtHR to adapt the protection granted under Article 8 ECHR to new circumstances and technological and

[317] *Kopp v Switzerland* App no 23224/94 (ECtHR 25 March 1999) para 53.
[318] Karin de Vries, 'Right to Respect for Private and Family Life' in Pieter van Dijk et al (eds) *Theory and Practice of the European Convention on Human Rights* (Intersentia 2018) 670.
[319] William Schabas, *The European Convention on Human Rights: A Commentary* (OUP 2015) 400, 401.
[320] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 509.
[321] *Niemietz v Germany* App no 13710/88 (ECtHR, 16 December 1992) para 32; *Halford v United Kingdom* App no 20605/92 (ECtHR 25 June 1997) para 44; Karin de Vries, 'Right to Respect for Private and Family Life' in Pieter van Dijk et al (eds) *Theory and Practice of the European Convention on Human Rights* (Intersentia 2018) 671.
[322] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 569, 570.
[323] Frederik Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting' (Doctoral thesis, Universiteit van Amsterdam 2015) 100 <https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5> accessed 8 February 2024.
[324] *Niemietz v Germany* App no 13710/88 (ECtHR, 16 December 1992) para 29; *Pretty v United Kingdom* App no 2346/02 (ECtHR 29 April 2002) para 61.

societal developments.[325] This dynamic approach to interpretation has been coined the 'living instrument doctrine'.[326] According to the ECtHR, it is crucial that the ECHR is interpreted and applied in a manner which renders its rights practical and effective, not theoretical and illusory.[327] Despite the fact that the living instrument doctrine is obvious in case law,[328] in a dispute concerning covert video surveillance of an employee being suspected of theft, the ECtHR included a sort of caveat with regard to technological developments. In this case, the ECtHR declared that there was a fair balance struck between the right to respect her private life under Article 8 and the employer's interest in the protection of its property rights and the public interest in proper administration of justice.[329] However, the ECtHR stated that 'The competing interests concerned might well be given a different weight in the future, having regard to the extent to which *intrusions* into private life are made possible by new, more and more sophisticated technologies'.[330] This clearly indicates that, depending on the intrusiveness of future technology, the balancing test could have a different outcome in the future. The living instrument doctrine also affects case law adopted by the CJEU. According to the CJEU, Article 8 ECHR and Article 7 EUCFR must be interpreted identically.[331] Furthermore, the EUCFR preamble reaffirms the rights as a result, inter alia, from the ECHR and the case law of the ECtHR and the CJEU.[332] Moreover, according to Article 52 (3) EUCFR, the 'meaning and scope' of the rights contained in the EUCFR and ECHR shall be the same, provided that these rights 'correspond'. This holds true for Article 8 of the ECHR and Article 7 of the EUCFR.

3.2 The fundamental right to data protection

Article 8 EUCFR grants everyone 'the right to the protection of personal data concerning him or her'. For the sake of brevity, I term this the *fundamental right to data protection*. There is no corresponding provision on data protection in the ECHR. However, ECtHR case law under the fundamental right to privacy gave rise to a right of data protection as well. Thus, the fundamental rights to privacy and protection of personal data are closely linked but not identical.[333] The Data Protection Directive[334] has

[325] Frederik Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting' (Doctoral thesis, Universiteit van Amsterdam 2015) 100 <https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5> accessed 8 February 2024.
[326] Alastair Mowbray, 'The Creativity of the European Court of Human Rights' (2005) Vol 5 Iss 1 Human Rights Law Review 57-59.
[327] *Christine Goodwin v United Kingdom*, App No 28957/95 (ECtHR 11 July 2002) para 74.
[328] Adapting the protection of Article 8 ECHR to technological developments, e.g. from letters to emails etc.
[329] *Köpke v Germany*, App No 420/07 (ECtHR 05 October 2010).
[330] *Köpke v Germany*, App No 420/07 (ECtHR 05 October 2010) emphasis added.
[331] Case C-400/10, *J. McB.* [2010] ECR I-582 para 53.
[332] Giovanni Carlo Bruno, 'The Importance of the European Convention on Human Rights for the Interpretation of the Charter of Fundamental Rights of the European Union' in Giuseppe Palmisano (ed) *Making the Charter of Fundamental Rights a Living Instrument* (Brill Publishing 2014) 90.
[333] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 223, 228; Herke Kranenborg, Commentary of Article 8 in Steve Peers et al (eds), *The EU Charter of Fundamental Rights* (Hart/Beck 2014) 229.
[334] 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 1995 L 281/31.

inspired Article 8 EUCFR; therefore, case law stemming from secondary EU law plays a role when interpreting Article 8 EUCFR.[335]

The following two sub-sections briefly discuss the differences between the fundamental right to privacy and data protection regarding the object and scope (Section 3.2.1) and introduce the principle of proportionality (Section 3.2.2) which plays an important role in EU data protection law.

3.2.1 Scope

The material scope of Article 8 EUCFR covers personal data, which entails all information on identified or identifiable natural persons.[336] Thus, the information protected by Article 8 EUCFR seems to be more extensive than the information covered by the right to privacy under Article 8 ECHR.[337] Additionally, the personal scope differs. The CJEU has excluded legal persons from the fundamental right to data protection,[338] whereas legal persons can rely on the fundamental right to privacy.[339] Unlike most of the other rights of the EUCFR, Article 8 contains several specifications that reflect key elements of the system of checks and balances.[340] Furthermore, Article 8 (2) EUCFR explicitly grants everyone '*right of access* to data which has been collected concerning him or her, and the *right to have it rectified*.'[341] These rights will be discussed in Section 3.3.4 below.

To what extent Article 8 EUCFR has a horizontal effect is unclear. It is argued that the provisions contained in the EUCFR do not directly create obligations for private parties because the provisions of the EUCFR are addressed solely to the institutions, bodies, offices, and agencies of the Union and to the Member States when implementing EU law.[342]As opposed to the fundamental right to privacy, there is extensive secondary EU law that regulates data protection. Secondary EU law will be discussed in Sections 3.3 and 3.4.

3.2.2 Principle of proportionality

As one of the general principles of EU law, the principle of proportionality[343] plays an important role in EU data protection law and has a decisive influence on the evaluation of whether a violation of the

[335] Herke Kranenborg, Commentary of Article 8 in Steve Peers et al (eds), *The EU Charter of Fundamental Rights* (Hart/Beck 2014) 223, 247.
[336] See Section 3.3.1.1 below for the term 'personal data'.
[337] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 225.
[338] Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 52, 53 and 87.
[339] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 225.
[340] Herke Kranenborg, Commentary of Article 8 in Steve Peers et al (eds), *The EU Charter of Fundamental Rights* (Hart/Beck 2014) 229.
[341] Emphasis added.
[342] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 225.
[343] Article 5 of the consolidated version of the Treaty Establishing the European Community [2006] OJ C321E/37.

right to data protection is justified.[344] The principle of proportionality is important not only in the context of Article 8 EUCFR, but also when interpreting EU secondary law as described in Sections 3.3 and 3.4. According to case law, the principle of proportionality 'requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it.'[345] Derogations and limitations in relation to the protection of personal data shall only apply in so far as is strictly necessary.[346]

According to EU law, the principle of proportionality has generally three components that involve the assessment of a measure's (i) suitability, (ii) necessity and (iii) proportionality stricto sensu.[347] Suitability assesses whether the measure concerned is suitable or relevant to the realisation of the goals it is aimed at meeting. Necessity raises the question whether the measure concerned is required to realise the goals it is aimed at. Proportionality stricto sensu examines non-excessiveness by determining whether the measure goes further than necessary to realise the goals it is aimed at meeting.[348] Necessity comprehends the so-called need-to-know principle and according to the CJEU, access to personal data must only be granted to authorities that have power in the specific field and not to other authorities.[349] Proportionality stricto sensu (iii) requires choosing the least onerous measure and the disadvantages caused by this measure must not be disproportionate to the aims pursued.[350] The CJEU has ruled that the Council and Commission did not comply with the principle of proportionality when requiring the publication of the names of all natural persons who were beneficiaries of agricultural funds and of the exact amounts received by those persons. It reached this conclusion because measures that would affect the fundamental right to data protection less adversely, but still would contribute to the aim pursued, had not been considered.[351]

3.3 General data protection regulation

Arguably, the most relevant and influential EU secondary data protection law is the General Data Protection Regulation (GDPR).[352] Regulations are binding legislative acts and must be applied in its entirety across the EU. With its 99 articles and 173 recitals, the GDPR must be regarded as a

[344] Charlotte Bagger Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) Vol 1 No 4 International Data Privacy Law 239-249.
[345] Joined Cases C–92/09 and C–93/09 *Schecke* [2010] ECR I-11063, para 74; *Vodafone and others* [2008] ECR I-188 para 51 and case law cited there.
[346] Case C-73/07 *Satamedia* [2008] ECR I-09831 para 56.
[347] Charlotte Bagger Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) Vol 1 No 4 International Data Privacy Law 239-249.
[348] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 148.
[349] Case C-524/06 Huber v Bundesrepublik Deutschland [2008] ECR I-724, para 61.
[350] Case C-331/*88 The Queen v Ministry of Agriculture* [1990] ECR I-4023, para. 13. See also Joined Cases C-133, C-300 and C-362/93 *Crispoltoni and others / Fattoria Autonoma Tabacchi* [1994] ECR 1–4863, para 40.
[351] Joined Cases C–92/09 and C–93/09 *Schecke* [2010] ECR I-11063, para 86.
[352] *EU General Data Protection Regulation* (GDPR): 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), OJ 2016 L 119/1.

comprehensive piece of legislation. It sets out rules relating to the protection of natural persons regarding the processing of their personal data and rules relating to the free movement of personal data. Article 1 (2) GDPR specifically refers to the objective of the GDPR to protect fundamental rights and freedoms of natural persons and, in particular, the right to the protection of personal data according to Article 8 EUCFR. The following Sections 3.3.1-3.3.4 will shortly elaborate on the most important concepts and provisions of the GDPR in light of the context of this thesis.[353] These sections cover material and personal scope (Section 3.3.1 and 3.3.2) as the well as data protection principles (Section 3.3.3) and the rights of the data subject (Section 3.3.4).

As explained in Section 2.1, AI refers to adaptive machines that can autonomously execute activities and tasks that require capabilities usually associated with humans. Although AI has the ability to make its *own* decisions and perform tasks on the designer's behalf,[354] the GDPR does not apply to AI as such because AI does not have a legal personality. Instead, the GDPR applies to controllers and processors deploying AI systems that process personal data. Therefore, not AI itself but its deployment by companies may cause legal problems. The use of an AI system falls under the scope of the GDPR only if both the material and personal scope are triggered.

3.3.1 Material scope

In essence, the GDPR applies to the processing of personal data wholly or partly by automated means and other than by automated means when the personal data form part of a filing system or are intended to form part of such a system.[355] Thus, whether the material scope of the GDPR is triggered depends on the following key terms: personal data (Section 3.3.1.1), special categories of personal data (Section 3.3.1.2) and processing (Section 3.3.1.3).

3.3.1.1 Personal data

Personal data are defined in Article 4 (1) GDPR as a concept with four elements: i) any information ii) relating to iii) an identified or identifiable iv) natural person. The first element reflects the aim of assigning a wide scope to the concept of personal data and potentially encompasses all kinds of information.[356] The form of the information appears to be irrelevant, as the information may be available 'in written form or be contained in, *for example*, a sound or image'.[357] The second element 'relating to' is also broadly interpreted by the CJEU and is satisfied 'where the information, by reason of its

[353] I do not elaborate on the territorial scope, specific obligations of controllers and on competent supervisory authorities and possible fines.
[354] Eduardo Alonso, 'Actions and agents' in Frankish Keith and Ramsey William M. (eds) *The Cambridge Handbook of Artificial Intelligence* (2014) 235, 236.
[355] Herke Kranenborg, Commentary of Article 2 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 66.
[356] Case C-434/16, *Nowak* [2017] ECR I-994 para 34.
[357] Joined Cases C-141/12 & C-372/12, *YS, M and S v Minister voor Immigratie, Integratie en Asiel* [2014] ECR I-2081, Opinion of AG Sharpston, para 45 (emphasis added).

content, purpose or effect, is linked to a particular person'.[358] What is decisive in whether information constitutes personal data depends on the third element, namely, whether the person concerned in fact is identified or identifiable. With respect to this element, a flexible approach is taken.[359] This is emphasised by the wording of Article 4 (1) and Recital 26 GDPR, in particular the references to 'singling out', 'directly or indirectly' and 'either by the controller or by another person'.[360] Regarding identification, Recital 26 states that account should be taken of 'all the means reasonably likely to be used'. According to the CJEU, this criterion would not be met if identification is prohibited by law 'or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost, and man-power, so that the risk of identification appears in reality to be insignificant'.[361] The last element of the concept of personal data makes clear that data on corporations or other legal/juristic persons[362] as well as artificial creatures (e.g. robots) are not protected by the GDPR. Overall, personal data seems to be a broad concept.[363]

3.3.1.2 Special categories of personal data

Article 9 (1) GDPR contains an exhaustive list of special categories of personal data, namely, 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.' Whereas Article 9 GDPR solely refers to the term 'special categories of personal data' (special data), Recitals 10, 51 and 53-54 also mention the term 'sensitive data'. According to the CJEU, the rationale to ensure enhanced protection for special data is based on their particular sensitivity. Processing of special data is liable to constitute a particularly serious risk of interference with fundamental rights to privacy and data protection.[364] According to the CJEU, the rationale is to prevent significant *risks* to data subjects arising from the processing of special data, regardless of any subjective element such as the controller's *intention*.[365] Thus, there is a higher standard of protection for special data because processing of them poses a greater risk to the fundamental rights of the data

[358] Case C-434/16, *Nowak* [2017] ECR I-994 para 35.
[359] Lee A. Bygrave, Luca Tosoni, Commentary of Article 4 (1) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 109.
[360] Ibid 110.
[361] Case C-582/14, *Breyer v Bundesrepublik Deutschland* [2016] ECR I-779, para 46.
[362] Lee A. Bygrave, Luca Tosoni, Commentary of Article 4 (1) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 111.
[363] Case C-487/21, *F.F.* [2022] ECR I-1000 para 26; Case C-434/16, *Nowak* [2017] ECR I-994 para 34; Purtova takes the view that, in the near future, everything will be or will contain personal data due to the rapid developments in technology. Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) Vol 10 Iss 1 Law, Innovation and Technology 40, 74-75 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 8 February 2024.
[364] Case C-184/20, *OT* [2022] ECR I-601, para 126; Case C-136/17, *GC and Others* [2019] ECR I-773 para 44; Recital 51 GDPR.
[365] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 paras 69-70; Case C-252/21, *Meta Platforms Inc.* [2022] ECR I-704, Opinion of AG Rantos para 41.

subject.[366] According to Recital 51 GDPR, this is due to the particularly sensitive nature of special data. Three of the categories of sensitive data listed in Article 9 (1) are further defined in the GDPR,[367] namely genetic data,[368] biometric data[369] and data concerning health.[370]

The definition of special categories of personal data must be interpreted broadly. The CJEU ruled that personal data which are liable to *indirectly* reveal special categories of personal data defined in Article 9 (1) GDPR are covered by the latter provision.[371] In this ruling, the CJEU followed the AG's opinion by stating that 'the verb "reveal" is consistent with the taking into account of processing not only of inherently sensitive data, but also of data revealing information of that nature *indirectly*, following an intellectual operation involving deduction or cross-referencing'.[372] Another case addresses the processing of special data in the context of websites and applications relating to Facebook users. Whether Article 9 (1) GDPR is applicable in this context depends, according to the CJEU, on the question 'whether the data collected, alone or by virtue of their association with the Facebook accounts of the users concerned, actually enable' to reveal one or more of the categories mentioned in Article 9 (1) GDPR. In certain cases, as pointed out by the CJEU, the mere act of visiting webites or the use of apps may already reveal information as referred to in Article 9 (1) GDPR.[373] Also, it is irrelevant whether a categorisation under Article 9 (1) GDPR is correct or not to fall under the scope of this provision.[374] Processing of special data is prohibited unless one of the exceptions listed in Article 9 (2) GDPR applies. These exceptions are exhaustive and must be interpreted restrictively.[375] In addition to one of the exceptions, processing of special data must always be supported by a legal basis[376] and comply with other provisions[377] of the GDPR.[378] As will be shown in Section 4.8, Article 9 GDPR is particularly relevant for the processing of arguably new types of sensitive personal data facilitated by AI (e.g., emotion data).

[366] Dara Hallinan et al, 'Neurodata and Neuroprivacy: Data Protection Outdated?' (2014) Vol 12 Iss 1 Surveillance and Society 67 <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata/neurodata4> accessed 8 February 2024.
[367] Ludmila Georgieva, Christopher Kuner Commentary of Article 9 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 374.
[368] Article 4 (13) GDPR.
[369] Article 4 (14) GDPR.
[370] Article 4 (15) GDPR.
[371] Case C-184/20, *OT* [2022] ECR I-601, paras 117-128.
[372] Case C-184/20, *OT* [2022] ECR I-601, paras 123, emphasis added; Case C-184/20, *OT* [2022] ECR I-601, Opinion of AG Pikamäe, para 85.
[373] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 paras 72-73.
[374] Ibid, para 69; See also Case C-252/21, *Meta Platforms Inc.* [2022] ECR I-704, Opinion of AG Rantos paras 39 and 40.
[375] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 para 76.
[376] According to Article 6 GDPR; see also European Data Protection Board, 'Guidelines 3/2019 on the processing of personal data through video devices' (29 January 2020) at 17.
[377] Such as principles for processing and other rules of the GDPR; see Recital 51 GDPR.
[378] Ludmila Georgieva, Christopher Kuner Commentary of Article 9 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 374, 376.

3.3.1.3 Processing

In Article 4 (2), the GDPR defines processing broadly by stating that processing refers to 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. In short, the definition of processing essentially covers any data processing operation and the use of the wording 'such as' indicates that the list entailed in the definition is not exhaustive. Processing might be further distinguished into automated and manual processing. The former refers to processing done by means of computing devices, and the latter to processing operations executed by humans without the use of computing devices.[379] It should be noted that manual processing falls only within the material scope of the GDPR if the personal data undergoing processing 'form part of a filing system or are intended to form part of a filing system'.[380]

Article 4 (6) GDPR defines a filing system as 'any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis'. Due to this broad definition, any sets of data grouped together in accordance with specific criteria making such data searchable and accessible without great difficulty are likely to be covered by the definition.[381] According to the CJEU, the requirement that data must be 'structured according to specific criteria' simply demands that personal data can be easily retrieved. In the words of the CJEU, personal data do not need to be 'contained in data sheets or specific lists in another search method, in order to establish the existence of a filing system'.[382]

3.3.2 Personal scope

The GDPR distinguishes between the different actors involved in data processing. These actors are the norm addressees of the GDPR, in essence, the entities that must comply with the GDPR, namely, 'controllers' and 'processors', and the individuals that are protected by the GDPR, the 'data subjects'. The latter are not defined in the GDPR, but Recital 14 indicates that the protection afforded by the GDPR applies to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. The definitions for the two actors having to comply with the GDPR, namely, controllers and processors, are introduced in Sections 3.3.2.1 and 3.3.2.2 respectively.

[379] Lee A. Bygrave, Luca Tosoni, Commentary of Article 4 (2) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 119,120.
[380] Article 2 (1) GDPR.
[381] Luca Tosoni, Commentary of Article 4 (6) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 143.
[382] Case C-25/17, *Jehova todistajat* [2018] ECR I-551 para 57-58.

3.3.2.1 Controller

Article 4 (7) GDPR defines controller as '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'.[383] It should be noted that the legal structure of the controller is irrelevant for being considered responsible for the legal obligations under the GDPR.[384] The concept of controller aims to primarily place responsibility for protecting personal data on the entity that actually exercises control over processing of personal data.[385] Regulatory guidance indicates that the concept of controller is functional and 'intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis'.[386] The decisive factor for controllership is the determination of purposes and means of processing personal data. The former relates to the reason and objective of the processing (why), and the latter is to be construed broadly as how processing is exercised, encompassing both technical and organisational elements. The criterion 'determine' can broadly be described as the ability to exercise influence.[387] As the definition in Article 4 (7) GDPR indicates, controllership may be shared. Where 'several operators determine jointly the purposes and means of the processing of personal data, they participate in that processing as [joint] controllers'.[388] Whereas a wide range of joint controllership arrangements are possible, it is often difficult in practice to delineate between joint controllers, separate controllers and other actors such as processors, especially in complex data processing that involve multiple parties.[389] Joint controllership does not presuppose that both controllers involved have access to the processed data.[390]

3.3.2.2 Processor

In addition to controllers, the GDPR imposes data protection obligations on processors defined as 'natural or legal person, public authority, agency or other body which processes personal data *on behalf of the controller*'.[391] As indicated in the definition, the role of the processor is inextricably linked to that of the controller. However, the processor is an entity that is legally separate from the controller and the relationship between these two actors is one of subservience: the processor must adhere to the instructions of the controller regarding the purposes and means of the processing.[392] Any

[383] Emphasis added.
[384] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 18.
[385] Luca Tosoni, Commentary of Article 4 (6) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 148.
[386] Art 29 Working Party, 'Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169, 16 February 2010) at 9.
[387] Lee A. Bygrave, Luca Tosoni, Commentary of Article 4 (7) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 150.
[388] Case C-40/17, *Fashion ID* [2019] ECR I-629 para 73.
[389] Lee A. Bygrave, Luca Tosoni, Commentary of Article 4 (7) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 152.
[390] Case C-210/16, *Wirtschaftsakademie* [2018] ECR I-388 para 38.
[391] Article 4 (8) GDPR emphasis added.
[392] Lee A. Bygrave, Luca Tosoni, Commentary of Article 4 (7) in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 160.

processor that goes beyond the mandate and instructions of the controller and takes part in determining the purposes and essential means of the processing will itself become a controller.[393] A variety of actors may be deemed processors,[394] including cloud service providers[395] and other external IT service providers or payroll service providers.[396]

3.3.3 Principles

Article 5 GDPR stipulates the principles that govern any processing of personal data. These principles provide the basis for the protection of personal data and some of them are further substantiated in other provisions of the GDPR.[397] The list of principles contained in Article 5 GDPR is exhaustive. In what follows, the principles lawfulness (Section 3.3.3.1), fairness (Section 3.3.3.2), transparency (Section 3.3.3.3), purpose limitation (Section 3.3.3.4), data minimisation (Section 3.3.3.5), accuracy (Section 3.3.3.6), storage limitation (Section 3.3.3.7), confidentiality (Section 3.3.3.8) and accountability (Section 3.3.3.10) will be introduced. In addition, I discuss data protection by design and default, as defined in Article 25 GDPR (Section 3.3.3.9). Strictly speaking, this provision is not a principle in the sense of Article 5 GDPR, but is inextricably linked to the data protection principles. For this reason, I introduce it in this section. The data protection principles discussed in this section will be used in Chapter 4 for further analyses of AI systems in the context of the GDPR.

3.3.3.1 Lawfulness

Lawfulness essentially requires that data processing respects all applicable legal requirements[398] and connotes proportionality in the balancing of interests of data subjects and controllers.[399] This principle is further substantiated in Article 6 GDPR. Processing is only lawful if at least one of the lawful bases listed in the latter provision applies. These exhaustive lawful bases are (i) consent of the data subject, (ii) performance of or entering into a contract, (iii) compliance with a legal obligation, (iv) vital interests of the data subject, (v) performance of a task in the public interest and (vi) the legitimate interest pursued by the controller or third party.[400] According to regulatory guidance, there is no normative hierarchy among the lawful bases[401] and, as indicated by the wording in Article 6 (1), a specific form of processing might be based on more than one lawful basis.

[393] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 20.
[394] Ibid.
[395] Art 29 Working Party, 'Opinion 05/2012 on Cloud Computing' (WP 196, 1st July 2012) at 8.
[396] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2 September 2020) at 14, 26.
[397] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 313.
[398] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 314.
[399] Lee A Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 148.
[400] Article 6 (1) lit a) to f) GDPR.
[401] Art 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014) at 10.

3.3.3.2 Fairness

Fairness requires that personal data have not been obtained or otherwise processed through unfair means, by deception or without the knowledge of the individual concerned.[402] Despite the fact that the fairness principle is a key tenet of EU data protection law and appears both in the EUCFR and GDPR, its role has thus been elusive[403] due to the lack of judicial guidance. However, both regulatory guidance[404] and regulatory enforcement at the EU level in the form binding decisions[405] adopted by the EDPB identify key elements of the fairness principle. These key elements are: autonomy of data subjects with respect to data processing, their reasonable expectations, ensuring power balance between controllers and data subjects, avoidance of deception, as well as possible adverse consequences of processing, and ensuring ethical and truthful processing.[406] In this sense, the fairness principle ensures 'that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject'.[407] Taking into account the text of Recital 39 GDPR, which stresses the link between transparency and fairness ('information to the data subjects [….] ensure fair and transparent processing'), absence of information will make processing unfair. However, fairness of processing means more than transparency[408] and has an independent meaning. This is confirmed by regulatory enforcement at the EU level. The principles of fairness, lawfulness and transparency are three *distinct* but intrinsically *linked* principles and fairness has an *independent* meaning.[409] The fairness principle focusses on proportionality in the balancing of interest of data subjects and controllers, and the latter have to take account of the reasonable expectations of data subjects when processing their personal data.[410]

[402] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 314.
[403] Damian Clifford, Jef Ausloos 'Data Protection and the Role of Fairness' (2018) Vol 37 No 1 Yearbook of European Law 130, 187, Milda Mačėnaitė, 'Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law' in Mor Bakhoum et al (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Nature 2018) 361.
[404] European Data Protection Board, 'Guidelines on Article 6(1)(b) GDPR' (Guidelines 2/2019, 8 October 2019), at 6; European Data Protection Board, 'Guidelines on Article 25 Data Protection by Design and Default' (Guidelines 4/2019, 20 October 2020), at 17 and 18.
[405] Article 65 GDPR.
[406] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022 paras 103, 219-220, 222-223, 226 478; Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), adopted on 5 December 2022 paras 106, 223-224, 226-227, 445; Binding Decision 5/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its WhatsApp service (Art. 65 GDPR) adopted on 5 December 2022.
[407] European Data Protection Board, 'Guidelines on Article 25 Data Protection by Design and Default' (Guidelines 4/2019, 20 October 2020), at 17 and 18.
[408] Winston J Maxwell, 'Principle-based regulation of personal data: the case of 'fair processing' (2015) Vol 5 No 3 International Data Privacy Law 205, 208.
[409] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022 paras 22, 477; Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), adopted on 5 December 2022 para 226, 444; Binding Decision 5/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its WhatsApp service (Art. 65 GDPR), adopted on 5 December 2022.
[410] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 147, 148.

3.3.3.3 Transparency

Recital 36 GDPR specifies the principle of transparency inherent in Article 6 (1) GDPR by requiring that it must be transparent to natural persons 'that personal data concerning them are collected, used, consulted or otherwise processed.'[411] It is further substantiated in Articles 12 through 14 GDPR in the form of obligations towards the controller to provide certain information to the data subject. In view of the EDPB, these provisions are the concretisation of the transparency principle, and violations of these provisions may also amount to the violation of the transparency principle itself.[412] Article 13 GDPR applies when personal data are collected from the data subject, and Article 14 applies when personal data have not been obtained from the data subject (e.g., third party controllers, data brokers, publicly available sources).[413] Information must be easily accessible, and when informing data subjects, the controller must use clear and plain language to make the information provided easy to understand.[414] It is important to note that the GDPR obliges controllers, amongst others,[415] to inform data subjects about the purposes of the processing for which the personal data are intended and the legal basis for the processing.[416] In the case of indirect collection, controllers must also inform data subjects about the categories of personal data that are undergoing processing.[417] The description of these categories should be precise enough to allow the data subject to grasp an overall understanding of the processing in view of the fairness and transparency principle.[418]

3.3.3.4 Purpose limitation

The purpose limitation principle enshrines two requirements: (i) personal data must be collected for specified, explicit and legitimate purposes and (ii) personal data must not be further processed for incompatible purposes.[419] The principle of proportionality is embodied in the purpose limitation principle by means of the requirement that personal data should be collected for specified and legitimate purposes. Thus, the purpose limitation principle seems to be intertwined with the proportionality principle because any assessment of the proportionality relies on the identification of a processing's purpose.[420] Specification requires that purposes must be determined at the very beginning of processing,

[411] Recital 39 GDPR.
[412] EDPB, 'Binding Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65 (1) lit a GDPR' (2021) paras 191, 193.
[413] Art 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP 260 rev.01, 11 April 2018) at 15.
[414] Recital 39 GDPR.
[415] For a full overview, see Article 13 and 14 GDPR as well as corresponding commentaries by Gabriela Zanfir-Fortuna, Commentary of Articles 13 and 14 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 413 et seq.
[416] Art 13 (1) lit c and Art 14 (1) lit c GDPR.
[417] Art 14 (1) lit d GDPR.
[418] Gabriela Zanfir-Fortuna, Commentary of Article 15 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 444.
[419] Case C-77/21 *Digi* [2022] ECR I-805 Opinion of AG Pikamäe para 28; Merel Elize Koning, 'The purpose and limitations of purpose limitation' (Doctoral thesis, Radboud University Nijmegen 2020) 58 < https://repository.ubn.ru.nl/bitstream/handle/2066/221665/221665.pdf?sequence=1&isAllowed=y > accessed 8 February 2024.
[420] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 148. Also, regulatory guidance on legitimate interest and purpose limitation is quite similar. See Art 29 Working Party, 'Opinion 06/2014 on the notion of

namely, at the time of collection of personal data. Thus, processing of personal data for undefined or unlimited purposes is unlawful.[421] The purpose specification requirement plays a central role because all the data protection principles introduced in Section 3.3.3 are based on it.[422] The purposes must be 'explicit', that is, clearly revealed, explained or expressed towards the data subjects concerned, to ensure an unambiguous understanding of the purposes of processing.[423] Legitimacy, another component of the purpose specification principle, arguably means that personal data should only be processed for purposes 'that do not run counter to ethical and social mores that are generally deemed appropriate to govern the relationship of the controller and data subject(s).'[424]

The principle of compatible use implies that a controller may process personal data for all purposes that may be considered compatible with the initial purposes. Article 6 (4) GDPR stipulates a series of criteria to determine whether further processing for a purpose other than the one for which personal data have been initially collected is 'compatible' with this initial purpose.[425] According to the CJEU, these criteria reflect the need for a concrete, coherent and sufficiently close link between the purpose of data collection and the further processing of the data and make it possible to determine that such further processing does not detract from the legitimate expectations as to the further use of their personal data.[426] Importantly, further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes is a priori not considered to be incompatible with the initial purposes provided that such processing is subject to appropriate safeguards.[427]

3.3.3.5 Data minimisation

The data minimisation principle enshrined in Article 5 (1) lit c GDPR stipulates that personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. Its requirements that personal data must be relevant and necessary impose limits on the amount of personal data that may be processed.[428] The stipulation that personal data must be 'relevant' and 'limited' in relation to the purposes for which they are processed gives expression to the

legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014) and Art 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, 2 April 2013).

[421] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 315.

[422] Merel Elize Koning, 'The purpose and limitations of purpose limitation' (Doctoral thesis, Radboud University Nijmegen 2020) 102 < https://repository.ubn.ru.nl/bitstream/handle/2066/221665/221665.pdf?sequence=1&isAllowed=y > accessed 8 February 2024.

[423] Art 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, 2 April 2013) at 39.

[424] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 155.

[425] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 315, 316.

[426] Case C-77/21 *Digi* [2022] ECR I-805 para 36; Case C-77/21 *Digi* [2022] ECR I-805 Opinion of AG Pikamäe paras 28, 59, 60.

[427] Article 89 GDPR.

[428] Asia Biega, Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' (2021) Technology and Regulation 44, 56 <https://arxiv.org/abs/2101.06203> accessed 8 February 2024.

principle of proportionality.[429] The latter is a requirement arising from settled case law.[430] According to Recital 39 GDPR, personal data should only be processed if the purposes cannot reasonably be fulfilled by other means. Anything exceeding the 'minimum' amount necessary will be considered excessive and violate the data minimisation principle. If the same results can be achieved through the processing of less personal data, the exceeding part of the processing is not necessary.[431] The data minimisation principle also plays a role with respect to the storage of personal data.[432] Furthermore, what is 'necessary' refers not only to the quantity, but also to the quality of the personal data processed.[433]

3.3.3.6 Accuracy

The GDPR states that the processing of personal data must be accurate and, where necessary, kept up to date.[434] Controllers have to rectify or erase all inaccurate data and must take every reasonable step to comply with the accuracy principle.[435] The term 'reasonable' arguably implies that it is legitimate for controllers to take into account cost and resource factors when deciding on measures to rectify or delete inaccurate data.[436]

The accuracy principle intends to protect the individual concerned from being irrationally or unfairly treated based on wrong and inaccurate representations.[437] According to regulatory guidance, accurate means 'accurate as to a matter of fact'.[438] What is required to assess the accuracy of the personal data depends on the context, namely, on the purpose of the processing.[439] Thus, the accuracy principle seems to be an undefined concept in EU data protection law because questions and definitions as to exactly how accurate personal data needs to be remain unaddressed.[440]

[429] Case C-439/19 *B* [2021] ECR I-504 para 98; Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 148.
[430] Cases C-92/09 and C-93/09, *Schecke* [2010] ECR I-662 paras 72 and 74; Case C-58/08, *Vodafone and others* [2008] ECR I-188 para 51.
[431] Asia Biega, Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' (2021) Technology and Regulation 44, 56 <https://arxiv.org/abs/2101.06203> accessed 8 February 2024.
[432] Case C-77/21 *Digi* [2022] ECR I-805 para 58.
[433] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 317.
[434] Art. 5 (1) lit d GDPR.
[435] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 317.
[436] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 164.
[437] Dara Hallinan, Frederik Zuiderveen Borgesius 'Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle' (2020) Vol 10 No 1 IDPL 1, 9.
[438] Art 29 Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain and inc v. Agencia Española de Protección De Datos (AEPD) and Mario Costeja González C-131/12' (WP 225, 26 November 2014), at 15. <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236> accessed 8 February 2024.
[439] Case C-434/16, *Nowak* [2017] ECR I-994 para 53.
[440] Dara Hallinan et al, 'Neurodata and Neuroprivacy: Data Protection Outdated?' (2014) Vol 12 Iss 1 Surveillance and Society 66, 67 <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata/neurodata4> accessed 8 February 2024.

3.3.3.7 Storage limitation

The storage limitation principle enshrined in Article 5 (1) lit d GDPR prohibits to store personal data in a form which permits identification of data subjects beyond the time necessary to achieve the purposes of processing. Storage for longer periods is permitted for or archiving purposes in the public interest, scientific or historical research purposes or statistical purposes provided that appropriate technical and organisational measures are implemented in order to safeguard the rights and freedoms of the data subjects.[441] The CJEU applied the storage limitation principle to a case where the controller 'stored personal data initially collected for other purposes in a testing and error correction database'. According to the CJEU, a controller cannot retain personal data in a database established for testing and error correction purposes for longer than what is necessary to conduct such testing and correct errors.[442]

3.3.3.8 Integrity and confidentiality

The integrity and confidentiality principle enshrined in Article 5 (1) lit f GDPR requires controllers to implement appropriate security measures to ensure that personal data are protected against unauthorised or unlawful processing and protected from accidental loss, destruction or damage.[443] Chapter IV of the GDPR further develops and substantiates this duty of security for both controllers and processors.[444] The measures taken should be commensurate with the risks involved in the processing.[445] I do not further elaborate on this principle because AI poses particular risks to information security. For instance, AI makes it easier for cybercriminals to penetrate systems without human intervention. Whereas such attacks could also compromise the protection of personal data, these attacks cause significant damage to companies whose systems were penetrated.[446] AI creates a 'cybercrime tsunami'[447] which merits dedicated research. However, such research does not fall within this thesis's scope.

3.3.3.9 Data protection by design and default

The concept of data protection by design and default enshrined in Article 25 GDPR does not appear under the principles for processing named in Article 5 of the GDPR. However, I mention it here under the principles because it is closely intertwined with them and important in the context of this thesis.[448] The concept of data protection by design and default obliges controllers to apply technical and

[441] Article 5 (1) lit e GDPR.
[442] Case C-77/21 *Digi* [2022] ECR I-805 paras 46-62.
[443] Article 5 (1) lit f GDPR.
[444] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 318.
[445] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 164; see also Article 32 GDPR.
[446] Eddie Segal, 'The Impact of AI on Cybersecurity' IEEE Computer Society <https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity> accessed 8 February 2024.
[447] Philip Treleaven et al, 'The Future of Cybercrime: AI and Emerging Technologies Are Creating a Cybercrime Tsunami' (2023) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507244 > accessed 8 February 2024.
[448] Because this concept seems to be particularly relevant for the use of new technologies, such as AI.

organisational measures 'that are designed to implement data protection principles'.[449] It also imposes a duty on controllers to integrate necessary safeguards into the processing of personal data to ensure that processing will meet its requirements and otherwise ensure the protection of data subjects' rights.[450] The 'by design' measures are both technical and organisational and embrace not simply the design and operation of software and hardware, but also business strategies and other organisational practices. The 'by default' requirements of Article 25 (2) GDPR are mainly concerned with results that guarantee data minimisation and confidentiality.[451] It is important to note that data protection by design and default measures must be taken at both the design and processing stage.[452]

3.3.3.10 Accountability

The accountability principle in Article 5 (2) GDPR states that the controller shall be i) responsible for compliance and ii) able to demonstrate compliance with all the previous principles mentioned in Article 5 (1) GDPR.[453] It is further developed in Article 24 GDPR and requires controllers to 'implement appropriate and effective measures to ensure and be able to demonstrate' that processing of personal data occurs in accordance with the rules set out in the GDPR.[454] It follows from the accountability principle itself and from CJEU case law that the burden of proof regarding the compliance with principles enshrined in Article 5 (1) GDPR lies with the controller.[455]

3.3.4 Rights

Chapter 3 of the GDPR provides the data subject with enforceable rights. The following sections will briefly elaborate on the scope of these rights. Note that the following sections do not discuss the information obligations that controllers must comply with, although these obligations are placed in Chapter III of the GDPR termed 'rights of the data subject'.[456] Thus, transparency requirements do technically not belong to the rights of data subjects and are therefore explained in Section 3.3.3.3 dealing with the transparency principle. I have chosen not to discuss notification obligations (Article 19 GDPR) and restrictions to data subject rights (Article 23 GDPR) contained in Chapter III GDPR. These provisions do not constitute enforceable data subject rights and thus fall out of the scope of this

[449] Article 25 GDPR.
[450] Lee A. Bygrave, Commentary of Article 25 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 576.
[451] Lee A. Bygrave, Commentary of Article 25 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 577.
[452] Article 25, Recital 78 GDPR.
[453] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 311.
[454] Art. 24 (1), Recital 74 GDPR.
[455] Case C-175/20 *'SS' SIA* [2022] ECR I-124 paras 77, 81.
[456] I do not take the view that something as a 'right to be informed' exists under the GDPR. Rather, controllers are obliged to comply with the transparency principle, which is further substantiated in articles 12-14 GDPR. In addition, the right to restriction of processing and notification obligation regarding rectification or erasure will be left out due to the lack of direct relevance for this thesis.

thesis. Additionally, I do not specifically address the right to restriction of processing according to Article 18 GDPR, but discuss it in the context of the right to object.

In what follows, the most prominent data subject rights will be introduced. These are the right of access (Section 3.3.4.1), the right to rectification (Section 3.3.4.2), the right to erasure (Section 3.3.4.3), the right to data portability (Section 3.3.4.4), the right to object (Section 3.3.4.5) and the right not to be subject to automated decision-making (Section 3.3.4.6). These data subject rights will be further analysed in the context of AI (Chapter 5).

3.3.4.1 Right of access

The right of access according to Article 15 GDPR provides the data subject with the right to demand in-depth information on processing going beyond the general information according to Articles 13-14 GDPR, which controllers must disclose to data subjects by default.[457] Article 15 GDPR enables data subjects to receive (i) confirmation of the processing, (ii) details about the processing and (iii) access to the personal data themselves, including a copy of the personal data.[458] The first element (i) simply includes a confirmation or denial of the controller that personal data of the data subject are being processed. Details to be provided according to element (ii) overlap with the information that must be disclosed under Articles 13 and 14 GDPR when personal data are collected or received. However, the details to be provided to the data subject under the right of access must be more precise and specifically address information about the personal data related to the person making the request.[459] Such details include, where applicable, information about automated decision-making.[460]

Element (iii) of the right of access obliges the controller to 'provide a copy of personal data undergoing processing'.[461] This aims to strengthen the position of the data subject.[462] The concept of 'copy' is not defined in the GDPR and therefore must be determined in line with usual meaning in everyday language as well as in the context of Article 15 GDPR. According to current linguistic usage, the term 'copy' refers to the 'reproduction or transcription' of an original.[463] Two well-known dictionaries define the notion as 'something that has been made to be exactly like something else'[464] or 'a thing that is made to be the same as something else, especially a document or a work of art'.[465] AG Pitruzella suggests interpreting the concept of copy as the '*faithful* reproduction in intelligible form of the

[457] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 150.
[458] Gabriela Zanfir-Fortuna, Commentary of Article 15 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 449.
[459] Ibid 463.
[460] Article 15 (1) lit h, Article 22 GDPR.
[461] Article 15 (3) GDPR.
[462] Case C-487/21, *F.F.* [2022] ECR I-1000 para 37; see also Opinion of AG Pitruzella para 69.
[463] Case C-487/21, *F.F.* [2022] ECR I-1000 para 21; see also Opinion of AG Pitruzella paras 28-30.
[464] See <https://dictionary.cambridge.org/dictionary/english/copy> accessed 8 February 2024.
[465] See <https://www.oxfordlearnersdictionaries.com/definition/english/copy_1?q=copy> accessed 8 February 2024.

personal data requested by the DS, in material and permanent form'.[466] He hesitated to clarify what is meant with 'faithful'. Dictionaries describe this notion as 'true and accurate; not changing anything'[467] and 'true or not changing any of the details, facts, style, etc. of the original'.[468] The CJEU followed AG Pitruzella's opinion. It ruled that a 'copy' refers to 'faithful reproduction or transcription' of an original. A purely general description of the data undergoing processing or a reference to categories of personal data does not correspond to that definition.[469] In addition, the right to obtain a copy includes not only personal data collected by the controller, but also information resulting from the processing of personal data, for instance, a credit score.[470] Therefore, the copy must enable the data subject to effectively exercise its right of access in full knowledge of all personal data undergoing processing, including personal data *generated* by the *controller*.[471] Article 15 (3) does not require the provision of a copy of the document but a copy of the personal data.[472] However, in some cases, controllers are required to recreate extracts from documents or even entire documents or extracts from databases containing personal that undergo processing to ensure that information is easy to understand, as required by Article 12 (1) GDPR.[473] In addition, Article 15 (3) GDPR does not provide the data subject with a right to obtain information regarding the criteria, models, rules or internal procedures (whether or not computational) used for processing the personal data.[474]

Importantly, the right of access may be restricted twofold, namely, in line with Article 23 GDPR and, more specifically, in accordance with Article 15 (4) GDPR. The latter only applies to element (iii) of the right of access. The right to obtain a copy of personal data shall not adversely affect the rights and freedoms of others,[475] 'including trade secrets or intellectual property and in particular the copyright protecting the software'.[476] The actual protection provided by the right of access must be determined contextually.[477] Rights, such as the right of access, may only be restricted when this constitutes a necessary measure to safeguard the rights and freedoms of others.[478] According to the CJEU, a balance will have to be struck in cases of conflict between right the right to obtain a full copy of personal data and rights and freedoms of others, including IP and trade secrets.[479]

[466] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 70.
[467] See <https://www.oxfordlearnersdictionaries.com/definition/english/faithful?q=faithful> and < accessed 8 February 2024.
[468] See < https://dictionary.cambridge.org/dictionary/english/faithful > accessed 8 February 2024.
[469] Case C-487/21, *F.F.* [2022] ECR I-1000 para 21.
[470] Ibid, para 26.
[471] Case C-487/21, *F.F.* [2022] ECR I-1000 para 21; see also the opinion of AG Pitruzella paras 45, 70.
[472] Note however that this depends on local guidance and local case law, arguably leading to 'unharmonized' results across the EU. In a recent case in the Netherlands, the court pointed out that the GDPR does not grant a right to obtain a copy of documents, but rather a right to obtain a copy of personal data. See Rechtbank Den Haag, *C/09/572633/HA RK 19-295* ECLI:NL:RBDHA:2019:13029 para 4.5.
[473] Case C-487/21, *F.F.* [2022] ECR I-1000 para 41.
[474] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 52.
[475] Article 15 (4) GDPR
[476] Recital 63 GDPR.
[477] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 536.
[478] Case C-434/16, *Nowak* [2017] ECR I-994 para 60.
[479] Case C-487/21, *F.F.* [2022] ECR I-1000 para 44.

The right of access is closely intertwined with other data subject rights because it allows data subjects to exercise these rights as noted by the CJEU.[480] According to the CJEU, the right of access 'is necessary, inter alia, to enable the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of his data by the controller and consequently to exercise' these rights.[481] Thus, according to the CJEU, the objective of the right of access is to guarantee the protection of the right to privacy with respect to data processing, and not to ensure 'the greatest possible transparency of the decision-making process of the public authorities and to promote good administrative practices by facilitating the exercise of the right of access to documents.'[482] Also, in another case, the CJEU stressed that the right to data protection is not designed to facilitate the exercise of the right of access to documents.[483] In conclusion, the main objective of Article 15 GDPR is to allow the data subject to be aware of processing, verify the lawfulness of the latter and enforce its rights as a data subject.[484]

3.3.4.2 Right to rectification

The right to rectification according to Article 16 GDPR enables the data subject to demand the controller to rectify inaccurate personal data and to have incomplete personal data completed. Thus, in addition to the rectification of inaccurate or false data, the data subject may add missing elements in order to complete personal data by providing a supplementary statement.[485] The CJEU held that the right to rectification may also be asserted in relation to written answers submitted by the candidate in a context of a professional examination, including comments made by an examiner.[486] However, the right to rectification must be interpreted teleologically. Obviously, the right to rectification should not result in situations where a candidate for a professional examination would be allowed to correct his answers in an exam retroactively[487] or an individual to rectify the content of a legal analysis in the context of an immigration case.[488] The question of whether personal data are accurate and complete must be assessed in light of the purpose for which the data was collected.[489] Regulatory guidance states that derived or inferred data constitute (new) personal data[490] and that the right to rectification applies not only to the 'input personal data' but also to 'output data'.[491] The term rectification implicitly relies upon the notion of verification in the sense that something may demonstrably be shown to

[480] Case C-434/16, *Nowak* [2017] ECR I-994 para 57; Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 65.
[481] Case C-487/21, *F.F.* [2022] ECR I-1000 para 35; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44.
[482] Ibid paras 46-47.
[483] Case C-28/08 P, *Bavarian Lager* [2010] ECR I-6055 para 49.
[484] Case C-487/21, *F.F.* [2022] ECR I-1000 para 35; see also Opinion of AG Pitruzella para 65.
[485] Cécile de Terwangne, Commentary of Article 16 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 473.
[486] Case C-434/16, *Nowak* [2017] ECR I-994 para 51.
[487] Ibid para 54.
[488] Joined Cases C-141/12 & C-372/12, *YS, M and S v Minister voor Immigratie, Integratie en Asiel* [2014] ECR I-2081, para 45.
[489] Case C-434/16, *Nowak* [2017] ECR I-994 para 53.
[490] Art 29 Working Party 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', (WP251rev.01, 6 February 2018) at 8-9.
[491] Ibid at 17-18.

be inaccurate or incomplete and consequently corrected by the individual concerned.[492] Indeed, AG Sharpston takes the view that 'only information relating to *facts* about an individual can be personal data.'[493] Such facts may be expressed in different forms, for example, a person's weight may be expressed objectively in kilogrammes or in subjective terms such as 'underweight' or 'obese'.[494] Demonstration of facts might be a straightforward task when the personal data in question is verifiable (such as a name, date of birth, email address or the weight of an individual).[495] With regard to inferred data, which are defined as products of probability-based processes,[496] it is generally impossible for data subjects to prove that such data are wrong without access to the tools used to infer the data.[497]

3.3.4.3 Right to erasure

The right to erasure in Article 17 GDPR is well known as 'the right to be forgotten' and was brought to great attention of the public by the Google Spain decision of the CJEU.[498] Under the right to erasure, the data subject may demand the controller to erase his or her personal data if the personal data (i) are no longer necessary in relation to the purposes for which they are processed, (ii) have been unlawfully processed, (iii) have to be erased for compliance with a legal obligation under EU or Member State law or (iv) have been collected based on a child's consent in relation to information society services.[499] The same applies when a data subject withdraws consent or objects to the processing of personal data.[500] However, the right to erasure is not an absolute right, as indicated by the exceptions enshrined in paragraph 3 of Article 17 GDPR. These exceptions apply regardless of the ground on which the erasure is based.[501] A controller must not comply with a data subject's request for erasure to the extent that processing is necessary for (i) exercising the right to freedom of expression and information; (ii) compliance with a legal obligation of the controller that requires processing by EU or Member State law and the performance of a task carried out in the public interest; (iii) reasons of public interest in the area of public health; (iv) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or (v) establishment, exercise or defence of legal claims.[502] The legal consequence of a successful request according to Article 17 (1) GDPR is the erasure of the personal

[492] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 548.
[493] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081, Opinion of AG Sharpston para 56.
[494] Ibid para 57.
[495] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 548.
[496] OECD Working Party on Security and Privacy in the Digital Economy JT03357584 (2014) <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en> accessed 8 February 2024.
[497] Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops' in Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press 2018) 115.
[498] Case C-131/12, *Google Spain* [2014] ECR I-317.
[499] Article 17 (1) lit a, d, e, f GDPR.
[500] Ibid lit b and c.
[501] Herke Kranenborg, Commentary of Article 17 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 482.
[502] Article 17 (3) GDPR. For regulatory guidance, see European Data Protection Board, 'Guidelines 05/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR part 1' (7 July 2020).

data.[503] The notion of 'erasure' is not defined in the GDPR, but it arguably refers to making data unusable in a way that prevents the controller, processor or any third party from processing the data by physically destroying or technically deleting the data.[504] Another legal consequence[505] is that the controller, if it has made the personal data public, is obliged to inform other controllers who are processing such data to erase any links to or copies of replications of the personal data.[506]

3.3.4.4 Right to data portability

Article 20 GDPR grants data subjects a right to indirect[507] and direct[508] data portability. Indirect data portability allows data subjects to receive their personal data and transmit them to another controller without interference from the original controller. Direct data portability enables data subjects to have their personal data transmitted directly from one controller to another.[509] As indicated in Recital 68 of the GDPR, the right to data portability 'should further strengthen the control' over personal data and is thus strongly related to the notion of control that dominated data protection reform efforts.[510] For the right to apply, three cumulative conditions have to be met: (i) the personal data have been provided directly by the data subject making the request, and processing is (ii) based on consent or a contract and (iii) carried out by automated means.[511] If one of the conditions is not met, the right cannot be invoked.[512] Condition (i) excludes personal data that is created by the controller, namely, personal data that is inferred or derived from personal data provided by the data subject.[513] Personal data like the 'online reputation' an individual develops in digital marketplaces based on customer reviews are likely excluded from the scope.[514] With regard to condition (ii), the right is limited to processing of personal data based on the lawful basis of consent[515] or performance of a contract.[516] Finally, condition (iii) excludes processing by nonautomated means.[517] When the data subject successfully invokes the right to data portability, the controller must provide the personal data in a 'structured, commonly used and machine-readable format.'[518] Recital 68 adds that the format should be interoperable and the requirement of a 'commonly used format', which is not defined in a recital or elsewhere in the GDPR,

[503] Meaning that one of the grounds in Article 17 (1) is triggered and no exception under Art. 17 (3) GDPR applies.
[504] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 161.
[505] Article 17 (2) GDPR.
[506] Herke Kranenborg, Commentary of Article 17 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 483.
[507] Article 20 (1) GDPR.
[508] Article 20 (2) GDPR.
[509] Stephanie Elfering, *Unlocking the Right to Data Portability* (Nomos 2019) 20.
[510] Inge Graef, Martin Husovec, Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' Vol 19 No 06 German Law Journal 1359, 1365.
[511] Article 20 (1) GDPR.
[512] Stephanie Elfering, *Unlocking the Right to Data Portability* (Nomos 2019) 23.
[513] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 10.
[514] Orla Lynskey, Commentary of Article 20 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 503.
[515] Article 6 (1) lit a GDPR.
[516] Article 6 (1) lit b GDPR.
[517] Stephanie Elfering, *Unlocking the Right to Data Portability* (Nomos 2019) 24.
[518] Article 20 (1) GDPR.

arguably refers to a format compatible with the state of the art at the time the request is made.[519] The right to data portability is not an absolute one, as Article 20 (4) indicates that this right shall not adversely affect the rights and freedoms of others. This provision arguably also covers intellectual property rights and trade secrets, as is the case with the right of access, which is closely related to the right to data portability.[520] It has been argued that this right, next to data protection law, also has a consumer and competition law dimension[521] and that this right does not fit well with the fundamental rights nature of data protection law.[522]

3.3.4.5 Right to object

Article 21 (1) GDPR confers on the data subject the right to object to processing 'on grounds relating to his or her particular situation'. Simultaneously, it imposes a duty on the controller to cease processing unless it can demonstrate 'compelling legitimate grounds for the processing', which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.[523] The term 'compelling' arguably means 'overwhelming' and thus requires that the rights and interests of the data subject are overridden in a strong, significant way.[524] Thus, the compelling legitimate grounds of the controller must be so important that the purposes of processing cannot be achieved without the processing that the data subject objected to.[525] The burden of proof that the conditions in Article 21 (1) are met lies with the controller, and any rejection to comply with a data subject's objection to the processing must be explained in the correspondence with the data subject.[526] When a data subject exercises the right to object, whether successful or not, the controller must immediately restrict the processing pursuant to Article 18 (1) lit d GDPR. Where the data subject's objection to processing has merit, the controller must no longer process personal data and has the obligation to erase them[527] 'without undue delay'.[528] If the data subject objects to processing for direct marketing purposes according to Article 21 (2) GDPR, including profiling related to direct marketing, there is no need to balance interests. This provision has an absolute character and therefore it is sufficient that the data subject simply objects to such processing.[529] Other than with an objection under

[519] Stephanie Elfering, *Unlocking the Right to Data Portability* (Nomos 2019) 21.
[520] Ibid 29, 30.
[521] Inge Graef, 'Blurring Boundaries of Consumer Welfare' in Mor Bakhoum et al (eds), *Personal data in competition, consumer protection and intellectual property law* (Springer 2018) 121-151.
[522] Inge Graef, Martin Husovec, Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' Vol 19 No 06 German Law Journal 1359, 1365.
[523] Article 21 (1) GDPR.
[524] Gabriela Zanfir-Fortuna, Commentary of Article 21 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 517.
[525] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 178.
[526] Gabriela Zanfir-Fortuna, Commentary of Article 21 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 517.
[527] Gabriela Zanfir-Fortuna, Commentary of Article 21 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 518.
[528] Article 17 (1) lit c GDPR.
[529] Gabriela Zanfir-Fortuna, Commentary of Article 21 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 518.

Article 21 (1) GDPR, the controller does not need to erase the personal data but is simply required to cease the processing of personal data for direct marketing purposes.[530] Where personal data are processed for scientific or historical research purposes or for statistical purposes, the data subject can object to such processing according to Article 21 (6) GDPR. However, when the processing referred to in this provision is necessary for the performance of a task carried out for reasons of public interest, such public interests prevail. In this case, the controller will be obliged to prove such a necessity.[531]

3.3.4.6 Right not to be subject to automated decision making

In Article 22 (1), the GDPR grants individuals 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'. According to the CJEU, the rationale of Article 22 GDPR is to protect data subjects effectively against 'the particular risks to their rights and freedoms associated with the automated processing of personal data'.[532] In academia, the nature of the right according to Article 22 (1) is subject to considerable disagreement.[533] The crucial question is whether Article 22 GDPR shall be interpreted as a general prohibition of automated decision-making (ADM) or if it must be interpreted as a right to be invoked, similar to a right to object.[534] In *SCHUFA*, the first case dealing with Article 22 GDPR, the CJEU interpreted this provision as a 'prohibition in principle',[535] thereby putting an end to this debate. This is in line with regulatory guidance,[536] AG Pikamäe's opinion[537] and my impressions from the oral hearing in this case.[538]

In order to apply, Article 22 (1) rests on three cumulative conditions: (i) a decision is made that is (ii) based solely on automated processing or profiling and (iii) has either legal effects or similarly significant effects.[539] Bygrave suggests that the use of the term 'including' profiling must be read as

[530] Article 21 (3) GDPR which states 'Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes'.
[531] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 179.
[532] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 57, 60.
[533] Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 530.
[534] Arguing that Article 22 is a right to be invoked by the data subject. See Luca Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation' (2021) Vol 11 Iss 2 International Data Privacy Law 145-162.
[535] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 52, 64.
[536] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018), at 9, 12, 19.
[537] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 31.
[538] Andreas Häuselmann, 'The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber' (European Law Blog, 20 February 2023) <https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/> accessed 8 February 2024.
[539] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 43; Opinion AG Pikamäe paras 33 and 36; Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 532.

equivalent to 'involving',[540] meaning that automated processing in the sense of Article 22 GDPR necessarily involves profiling.[541] In other words, profiling is seen as a necessary element of automated processing. However, such an interpretation is not undisputed because the term 'including' could also simply imply that automated processing *may* involve profiling. AG Pikamäe seems to support the latter interpretation. In his view, profiling is a subcategory of automated processing,[542] which implies that automated processing according to Article 22 (1) GDPR may involve profiling, but also covers other forms of automated processing. Furthermore, the regulatory guidance correctly points to the different concepts of 'ADM' and 'profiling': ADM has a different scope than profiling,[543] but may partially overlap with or result from the latter. In addition, ADM may be made with or without profiling; and profiling can take place without ADM.[544] Unfortunately, the CJEU did not address this question explicitly in *SCHUFA*, arguably because it was clear that the automated establishment of a credit score value constitutes profiling.[545] For this thesis, I interpret the reference to profiling in line with AG Pikamäe's opinion in *SCHUFA*[546] and regulatory guidance. This interpretation also matches with the rationale of Article 22 GDPR according to the CJEU, namely effective protection against risks associated with *automated processing* of personal data.[547]

The GDPR does not define the term decision contained in Article 22 (1) GDPR. However, the CJEU interprets this term broadly based on Recital 71 GDPR which also refers to 'measures'.[548] Following AG Pikamäe's opinion,[549] the CJEU ruled that a decision covers many acts which may affect individuals in several ways, including the automated establishment of a score value.[550] Bygrave suggests that a decision as required by condition (i) covers a wide range of situations and should be viewed in a fairly generic sense, provided it is formalised so that it can be distinguished from other stages that prepare, support or complement decision-making.[551] According to AG Pikamäe, the term decision implies a 'view' or 'opinion' on a particular matter from an etymological point of view. It is not necessary for the decision to have a specific form; the *effect* that the decision has on the data subject is *decisive*.[552]

[540] Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 252.
[541] Isak Mendoza, Lee A Bygrave, 'The Right Not to be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou et al (eds) *EU Internet Law: Regulation and Enforcement* (Springer International 2017) 91.
[542] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 33.
[543] Defined in Article 4 (4) GDPR.
[544] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) at 8.
[545] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 47.
[546] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 33.
[547] The CJEU referred to automated processing and not 'only' profiling, Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 57. Also, in paras 53, 62, 68 and 72 the CJEU mentions automated processing, not profiling.
[548] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 44, 45.
[549] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe paras 38, 42.
[550] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 46.
[551] Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 532.
[552] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe paras 37, 43.

The second condition (ii) means the absence of meaningful human involvement (or better: influence) in the decision process. Meaningful human involvement requires that it be carried out by a person who is competent or authorised to change a decision. Routinely applying automated decisions without any actual influence on the result (e.g., rubber-stamping automated decisions) would not be regarded as human involvement.[553] The last condition (iii) requires that the decision changes, shapes or otherwise determines an individual's rights or duties or has consequences that have a serious adverse impact.[554] Legal effects under condition (iii) means that the decision affects an individual's legal rights, such as the freedom to associate with others, vote in an election or take legal action. It also involves decisions that affect a person's legal status or rights under a contract (for example, cancellation of a contract or entitlement to social benefits).[555]

Naturally, defining what meets the threshold of 'significant effects' is more difficult. According to AG Pikamäe, these significant effects may be of economic and social nature and relate to severe consequences for freedoms and autonomy. They include adverse effects resulting from a negative score value, which significantly restricts the data subject in exercising its freedoms or even stigmatises the data subject.[556] The CJEU went a bit less far, but confirmed that the automated establishment of a probability value (credit score) meets the threshold of 'significant effects'.[557] The application of this threshold will arguably vary depending on the attributes and sensibilities of the data subject concerned.[558] Regulatory guidance indicates that the threshold may be met when the decision has the following: the potential to significantly affect the circumstances, behaviour or choices of the individual; a prolonged or permanent impact; or, in its most extreme form, the risk of leading to the exclusion or discrimination of individuals.[559]

According to Article 22 (2) GDPR, the prohibition of ADM[560] does not apply in three alternative sets of circumstances, namely, when ADM is necessary in the context of a contract, based on a statutory authority or based on consent. However, data subjects will always have the right to demand human review, to express their point of view and to contest the decision, except when ADM is based on statutory authority.[561] Whether Article 22 (3) requires controllers to provide data subjects with a right

[553] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018), at 20, 21.
[554] Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 534.
[555] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018), at 21.
[556] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe paras 38, 39, 42, 43.
[557] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 48-50.
[558] Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 534.
[559] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018), at 21.
[560] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 52, 53, 64.
[561] Article 22 (3) GDPR; Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 534.

of ex-post explanation (after the decision is adopted) has been subject to scholarly debate.[562] However, when considering the accountability, fairness and the transparency principles and related provisions (e.g. to provide 'meaningful information about the logic involved' in ADM) there seems to be solid ground for a right for ex-post explanation.[563] Article 22 (4) further prohibits ADM based on special categories of personal data unless such ADM is necessary for reasons of substantial public interest[564] or the data subject has provided explicit consent.[565]

3.4 ePrivacy Directive

The provisions of the ePrivacy Directive (ePD)[566] aim to 'particularise and complete'[567] the GDPR[568] in the electronic communications sector.[569] EU Directives, as opposed to EU Regulations, must be implemented in national legislation of EU Member States. This can lead to differences within the different EU Member States.[570] Whereas both the GDPR and the ePD have the object of protecting fundamental rights and freedoms,[571] the GDPR sets general rules for the processing of personal data, and the ePD regulates the fundamental right to privacy *and* data protection in the electronic communications sector.[572] Thus, in accordance with the principle lex specialis derogate legi generali,[573] provisions of the ePD that specifically regulate processing of personal data in the electronic communications sector take precedence over the general provisions of the GDPR.[574] However, this applies only where the material scope of both laws is triggered.[575] The relationship between the GDPR and ePD is

[562] Denying the existence of such a right: Sandra Wachter, Brent Mittelstadt, Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) Vol 7 Iss 2 IDPL 76-99; most scholars however disagree: Andrew Selbst, Julia Powles, 'Meaningful information and the right to explanation' (2017) Vol 7 Iss 4 IDPL 233-242; Giancludio Malgieri, Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) Vol 7 Iss 4 IDPL 243-265; Isak Mendoza, Lee A. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling', in Synodinou Tatiana-Eleni et al (eds), EU Internet Law: Regulation and Enforcement (Springer 2017) 77.
[563] Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 538.
[564] Article 9 (2) lit g GDPR.
[565] Article 9 (2) lit a GDPR.
[566] 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 OJ L 201/27 further on referred to as 'ePrivacy Directive' as amended by Directive 2009/136/EC.
[567] Article 1 (2) ePrivacy Directive.
[568] Initially Data Protection Directive 95/46/EC.
[569] Tijmen H.A. Wisman, 'Privacy, Data Protection and E-Commerce' in Arno L. Lodder, Andrew D. Murray (eds) *EU regulation of e-commerce. A commentary* (Elgar 2017) 369.
[570] In this thesis, I do not elaborate on the relevant Member State laws.
[571] In the case of the GDPR, the fundamental right to the protection of personal data (Article 1 para 2 GDPR), and in the case of the ePrivacy Directive, both the fundamental right to privacy (Recital 12) and data protection (Recital 2). Note that Directive which amended the ePrivacy Directive also refers to the fundamental right to privacy and confidentiality (Recital 51) and the fundamental right to the protection of personal data (Recital 56).
[572] Christina Etteldorf, 'EDPB on the Interplay between the ePrivacy Directive and the GDPR' (2019) Iss 5 No 2 European Data Protection Law Review 224, 226.
[573] Joined Cases *T-60/06 RENV II and T-62/06 RENV II* [2016] ECR II-233 para 81.
[574] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (Opinion 5/2019, 12 March 2019), at 17.
[575] Christina Etteldorf, 'EDPB on the Interplay between the ePrivacy Directive and the GDPR' (2019) Iss 5 No 2 European Data Protection Law Review 224, 226.

governed by Article 95 and Recital 173 of the GDPR. Note that the proposed ePrivacy Regulation,[576] which is supposed to repeal the ePD, is still subject to political negotiations. I will discuss this proposal to a limited extent in Sections 4.8.3, 4.9, 6.4.2, 6.4.3.

The following sections outline the material scope (Section 3.4.1) and the personal scope (Section 3.4.2) of the ePD. The last section elaborates on the provisions of the ePD that specifically regulate the use of certain types of information and the processing of personal data (Section 3.4.3).

3.4.1 Material scope

The ePD applies to the processing of personal data in connection with the provision of publicly available electronic communications services ('ECS') in public communications networks in the EU.[577] To establish what constitutes an ECS requires some effort as the ePD refers to the Framework Directive[578] which, in the context of the modernisation of the EU's telecom framework, has been repealed by the European Electronic Communications Code ('EECC').[579] The latter introduces a new definition of ECS and because Article 125 and Annex XII of the EECC specifically require that any cross reference to the repealed Framework Directive is construed to refer to the EECC, the scope of the ePD has been extended. The new definition of ECS covers Internet access services, interpersonal communications services and services consisting wholly or mainly in the conveyance of signals.[580] It also includes over-the-top (OTT) services delivering content over the Internet such as VoIP[581] solutions, messaging services and web-based email services which are functionally equivalent to the more traditional voice telephony and text message services.[582] Under the previous definition of ECS, purely Internet-based VoIP solutions were not covered and did therefore not fall under the scope of the ePD.[583] According to CJEU case law, to fall within the scope of an ECS, a service must include the *conveyance of signals.*[584] All that matters concerning the conveyance of signals is that a service provider is *responsible* vis-à-vis the end-users for *transmission* of the *signal* which ensures that they are supplied with the service to which they have subscribed.[585] In the case of web-based services, it is the *Internet Access Provider* (IAP) and the *operators* of the *various networks* of which the *open Internet* is constituted

[576] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final 'Proposal ePrivacy Regulation'.
[577] Article 3 (1) ePrivacy Directive.
[578] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services OJ L 108 further on 'Framework Directive'.
[579] Directive (EU) 2018/1972 of the European Parliament establishing the European Electronic Communications Network OJ L 321/36 further on 'EECC'.
[580] Article 2 (4) EECC.
[581] VoIP solutions, for example, enable individuals to call via computer without the call being routed on to a number in the regular telephony numbering plan.
[582] Recital 15 EECC.
[583] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulaton' (2015) European Commission 36 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.
[584] Case C-193/18, *Google LLC* [2019] ECR I-498 para 32.
[585] Case C-475/12, *UPC* [2014] ECR I-285 para 43.

that convey the signals necessary for the functioning of web-based services.[586] It is also common understanding that providers of web-based services (e.g. Gmail) somehow participate in the conveyance of signals, for example, by means of uploading data packets to the open Internet or by splitting messages into data packets. However, this is not sufficient to be regarded as an ECS consisting 'wholly or mainly in the conveyance of signals on electronic communications networks'.[587] In essence, the ePD applies when the following cumulative conditions are met: (i) there is an ECS[588] which is (ii) offered over an electronic communications network[589] and the service and network are (iii) publicly available[590] and (iv) offered in the EU.[591] In addition, the material scope of the ePrivacy extends to the storage of information or gaining access to information already stored in the terminal equipment of a subscriber or user[592] (including cookies and other tracking technologies) and unsolicited communications (including direct marketing).[593]

3.4.2 Personal scope

As indicated by its material scope, most of the provisions of the ePD only apply to providers ECS.[594] Certain provisions of the ePD are nevertheless applicable to providers of information society services.[595] Article 5 (3) ePD as indicated by regulatory guidance applies to every entity that places on or reads information from terminal equipment including smart devices[596] and regardless of the nature of the entity.[597] This includes particularly websites operators that place cookies[598] and apps that are installed on the end-user device and access data stored on the device.[599] In addition, Article 13 ePD applies to any business, including website operators, which sends unsolicited electronic mail for direct marketing purposes.[600]

[586] Case C-193/18, *Google LLC* [2019] ECR I-498 para 36.
[587] Ibid.
[588] As defined in Article 2 (4) EECC.
[589] As defined in Article 2 (1) EECC.
[590] A service available to all members of the public on the same basis.
[591] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (Opinion 5/2019, 12 March 2019), at 10.
[592] Article 5 (3) ePrivacy Directive.
[593] Article 13 ePrivacy Directive.
[594] Article 29 Working Party, 'Opinion 3/2013 on apps on smart devices' (WP 202, 27 February 2013) at 7.
[595] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulaton' (2015) European Commission 9 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.
[596] Including smartphones, tablets and smart TVs.
[597] Article 29 Working Party, 'Opinion 3/2013 on apps on smart devices' (WP 202, 27 February 2013), at 7.
[598] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (Opinion 5/2019, 12 March 2019), at 11.
[599] Article 29 Working Party, 'Opinion 3/2013 on apps on smart devices' (WP 202, 27 February 2013), at 14.
[600] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (Opinion 5/2019, 12 March 2019), at 11.

The ePD protects users who are individuals, meaning 'any natural person using a publicly available electronic communications service, for both private and business purposes, without necessarily having subscribed to this service'[601] as well as subscribers who are legal persons.[602] In this sense, the ePD complements the GDPR, as the latter does not provide protection to legal persons.

3.4.3 Specific requirements

This section elaborates on provisions of the ePD that specifically regulate the use of certain types of information and the processing of personal data. Where provisions of the ePD require consent, such consent must meet the conditions for obtaining consent according to the GDPR.[603] The CJEU already interpreted the notion of consent as required in Article 5 (3) ePD in the light of the GDPR.[604]

In what follows, I discuss provisions enshrined in the ePD with particular relevance in the context of AI. These are confidentiality of communications (Section 3.4.3.1), information stored in terminal equipment (Section 3.4.3.2) and location data (Section 3.4.3.3).

3.4.3.1 Confidentiality of communications

Article 5 (1) ePD protects the confidentiality of communications and the related traffic data.[605] It prohibits listening, tapping, storage or other types of interception and surveillance by persons other than users. Interception of communication is allowed if the user provided consent or if technical storage is necessary for the conveyance of communication.[606] Article 5 (2) ePD provides for the so-called business exception[607] and states that the protection of confidentiality shall not affect recordings for the 'purpose of providing evidence of a commercial transaction or of any other business communication'.

3.4.3.2 Information stored in terminal equipment

Article 5 (3) ePD regulates the storage of information, or gaining access to information already stored, in the terminal equipment of a subscriber or user. According to regulatory guidance, terminal equipment must be interpreted broadly, including smart devices such as smartphones, tablets, smart TVs

[601] Article 2 lit a ePrivacy Directive.
[602] Article 1 (2) ePrivacy Directive.
[603] Article 94 GDPR; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) at 6.
[604] Case C-673/17 *Planet 49 GmbH* [2019] ECR I-801 paras 60-65.
[605] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulaton' (2015) European Commission 10 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.
[606] Article 5 (1) ePrivacy Directive; Tijmen H.A. Wisman, 'Privacy, Data Protection and E-Commerce' in Arno L. Lodder, Andrew D. Murray (eds) *EU regulation of e-commerce. A commentary* (Elgar 2017) 371.
[607] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulaton' (2015) European Commission 11 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.

etc.[608] Article 5 (3) ePD does not require the processing of personal data.[609] Recital 24 ePD outlines that information stored on terminal equipment is 'part of the private sphere of the users requiring protection' and 'may seriously intrude upon the privacy of these users'. The legislator has amended the ePD in 2009 to make consent a requirement for storage of such information. Thus, for information to be stored in terminal equipment, whether the information constitutes personal data or not, requires the consent of the user or subscriber.[610] If placing and retrieving information through cookies or similar means is also considered to constitute processing of personal data, the GDPR applies in addition to Article 5 (3) ePD.[611] Because the provision in the ePD constitutes a lex specialis, it prevails over the GDPR and thus, consent of the user or subscriber is needed meaning that the controller cannot rely on the full range of possible lawful bases provided by Article 6 GDPR.[612] However, there are two exceptions where prior consent is not required. These are technical storage for the sole purpose of carrying out the transmission of a communication and the provision of an information society service that is explicitly requested by the user or subscriber.[613]

3.4.3.3 Location data

Article 9 ePD governs the processing of location data *other*[614] than traffic data through a public communications network or publicly available ECS.[615] This provision regulates only a fraction of location based services and thus services that are offered to members of a private network are not subject to the ePD. Therefore, Article 9 does not apply to location data transmitted through enterprise networks aimed at a private user group, or data collected and transmitted through infrared signals or GPS signals in combination with a private wireless network.[616] In addition, regulatory guidance states that 'the ePrivacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network'.[617] As

[608] Article 29 Working Party, 'Opinion 3/2013 on apps on smart devices' (WP 202, 27 February 2013) at 7.
[609] Case C-673/17 *Planet 49 GmbH* [2019] ECR I-801 para 69.
[610] Article 5 (3) ePrivacy Directive as amended by Directive 2009/136/EC.
[611] Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' (WP 171, 22 June 2010) at 9.
[612] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (Opinion 5/2019, 12 March 2019), at 14.
[613] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulaton' (2015) European Commission 13 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.
[614] Thus, location data which is also traffic data are governed by Article 6 ePrivacy Directive (see Recital 35).
[615] Tijmen H.A. Wisman, 'Privacy, Data Protection and E-Commerce' in Arno L. Lodder, Andrew D. Murray (eds) *EU regulation of e-commerce. A commentary* (Elgar 2017) 376.
[616] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulation' (2015) European Commission 14 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.
[617] Article 29 Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices' (WP 185, 16 May 2011) at 9.

a result, processing location data via techniques such as Wi-Fi network proximity or IP-address databases is not covered by Article 9 ePD.[618]

Article 9 ePD allows processing of location data when they are (i) anonymous or (ii) when the user or subscriber provided consent to the extent and for the duration necessary for the provision of value-added services. Anonymisation is a controversial concept[619] considering that technology is rapidly evolving and thus facilitates better (and quicker) identifiability of individuals.[620] This seems to be particularly relevant since the exception does not restrict the processing of anonymised location data to specific purposes.[621]

3.5 Conclusions

Chapter 3 examined *Subquestion 2:* What is the current EU legal framework? The fundamental rights to privacy and the protection of personal data enshrined in the EUCFR as well as the GDPR and ePD together form the '*current legal framework*'.

The fundamental right to *privacy* according to Article 7 EUCFR protects everyone's 'right to respect for his private and family life, his home and communications'. The fundamental right to *data protection* enshrined in Article 8 EUCFR grants everyone 'the right to the protection of personal data concerning him or her'. It applies to personal data, which entails all information on identified or identifiable natural persons. The two fundamental rights[622] are closely linked, but not identical.[623] Information protected by the fundamental right to data protection seems to be more extensive as opposed to the information covered by the fundamental right to privacy.[624] In addition, the personal scope differs. Legal persons are excluded from the fundamental right to data protection[625] whereas legal persons can rely on the fundamental right to privacy.[626] Both fundamental rights are further

[618] Eleni Kosta, Jos Dumortier, 'ePrivacy Directive: Assessment of transposition, effectiveness and compatibility within the proposed Data Protections Regulation' (2015) European Commission 14 <https://research.tilburguniversity.edu/en/publications/eprivacy-directive-assessment-of-transposition-effectiveness-and-> accessed 8 February 2024.
[619] Tijmen H.A. Wisman, 'Privacy, Data Protection and E-Commerce' in Arno L. Lodder, Andrew D. Murray (eds) *EU regulation of e-commerce. A commentary* (Elgar 2017) 376.
[620] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) Vol 10 Iss 1 Law, Innovation and Technology 40, 74-75 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 8 February 2024.
[621] As opposed to exception of consent, which only allows processing for the provision of value added services.
[622] Note that the human right to respect for private and family life according to Article 8 ECHR and related ECtHR case law highly influence the interpretation of the two fundamental rights.
[623] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 223, 228; Herke Kranenborg, Commentary of Article 8 in Steve Peers et al (eds), *The EU Charter of Fundamental Rights* (Hart/Beck 2014) 229.
[624] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 225.
[625] Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 52, 53 and 87.
[626] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 225.

substantiated in EU secondary law. The most relevant legislation in EU secondary law are the GDPR and the ePD.

The *GDPR* is the most comprehensive piece of legislation in data protection law and arguably also the most influential one. It contains rules relating to the protection of natural persons regarding the processing of their personal data, as well as rules aimed at facilitating the free movement of personal data. The most important provisions of the GDPR are the principles contained in Article 5 GDPR, as well as the rights of data subjects enshrined in Chapter III GDPR.

Provisions of the *ePD* aim to 'particularise and complete'[627] the GDPR[628] in the electronic communications sector.[629] Whereas both the GDPR and the ePD have the object of protecting fundamental rights and freedoms, the GDPR sets general rules for the processing of personal data. The ePD regulates the fundamental right to privacy *and* data protection in the electronic communications sector.[630] In accordance with the principle lex specialis derogate legi generali,[631] provisions of the ePD that specifically regulate processing of personal data in the electronic communications sector prevail over the general provisions of the GDPR.[632] The most important provisions of the ePD in light of AI are confidentiality of communications, information stored in terminal equipment and location data.

[627] Article 1 (2) ePrivacy Directive.
[628] Initially Data Protection Directive 95/46/EC.
[629] Tijmen H.A. Wisman, 'Privacy, Data Protection and E-Commerce' in Arno L. Lodder, Andrew D. Murray (eds) *EU regulation of e-commerce. A commentary* (Elgar 2017) 369.
[630] Christina Etteldorf, 'EDPB on the Interplay between the ePrivacy Directive and the GDPR' (2019) Iss 5 No 2 European Data Protection Law Review 224, 226.
[631] Joined Cases *T-60/06 RENV II and T-62/06 RENV II* [2016] ECR II-233 para 81.
[632] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (Opinion 5/2019, 12 March 2019) at 17.