Uncontrollable: Data subject rights and the data-driven economy

Ursic, H.

5. THE RIGHT TO INFORMATION

5.1. Introduction

This chapter addresses the right to information, the cornerstone of the system of control rights under the GDPR. In the EU DPD, the right to information was separated from the rest of the provisions on data subject rights. However, the GDPR altered the directive's structure and made the right to information a constituent part of Chapter 3 (data subject rights).

The right to information is *primus inter pares* among the data subject rights. Formally, all the rights are deemed equal, but in practice the right to information stands out as it exemplifies the principle of transparency and represents the focal point for all other data subject rights. Without the necessary information, a data subject cannot meaningfully participate in the data economy, nor can she exercise her other control rights.[623] The story of Max Schrems is telling. Schrems, who became famous after having sued Facebook for not complying with EU privacy laws, used the right to information and access to go after the social media giant.[624] If Schrems had had no knowledge about the amount and quality of data which Facebook had processed about him, he would have had difficulty disagreeing with its data processing practices in first place. This view finds support in the CJEU's ruling in *Bara*: *'The right to information is the precondition for other rights: the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed […] and their right to object to the processing of those data […].'*[625]

By exploring the GDPR provisions on the right to information and the corresponding parts of the ePrivacy directive,[626] this chapter seeks to answer the fourth research question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* While this research question refers to data subject rights as a whole, in this chapter the scope is narrowed down to what is necessary to understand the right to information, and to assess the vigour of control that it offers to individuals.

This chapter starts with a brief discussion of the normative bases of the right to information in section 5.2. Section 5.3. then turns to three aspects of the right: the content, the format, and the timing required to convey the necessary information. Special attention is given to the right to explanation of automated decision-making, which is to some extent a novel concept. In addition to the GDPR's provisions on the right to information, ePrivacy law contains some specific rules on the right to information in the electronic communications sector. These are explained in section 5.4. Throughout

---

[623] Max Schrems received knowledge about Facebook's data processing when he was studying in the US and listening to a lecture by a Facebook privacy counsel. Helena Ursic, 'How a study exchange triggered a CJEU landmark case' (*Leiden Law Blog,* 20 October 2015) <http://leidenlawblog.nl/articles/how-a-study-exchange-triggered-a-cjeu-landmark-decision> accessed 5 June 2018.

[624] Cyrus Farivar, 'How one law student is making Facebook get serious about privacy' *ArsTechnica* (15 November 2012, <https://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/2/> accessed 5 June 2018.

[625] C-201/14 *Bara and Others* [2015] ECLI:EU:C:2015:638. Also see the Opinion of AG Cruz Villalón in the same case.

[626] I analyse both the currently valid ePrivacy Directive and the proposed ePrivacy Regulation. The focus is on the directive. When I refer to the regulation, I will mention it specifically.

the chapter, the positive and negative implications of the data-driven economy for the right to information are carefully considered. Based on the findings, section 5.5. provides an answer to the control-related research sub-question.

5.2. The link to fundamental values

The GDPR's version of the right to information stems from some fundamental values: privacy, autonomy, transparency, and fairness.

The right to information is particularly strongly intertwined with transparency as a fundamental value. In both the private and the public sector, transparency serves the objectives of legitimate governance. More transparency regarding the decisions of a decision-making body, either of the government or of a powerful company, encompasses equality or, in other words, the *balance of powers*.[627] Considering strong information asymmetries in relation to personal data processing on the data-driven markets,[628] it quickly becomes clear why the ideas behind transparency and other human rights must apply equally to private sector actors.[629]

As Chapter 2 showed, complex data flows and automated (i.e. algorithmic) decision-making have become standard elements within the data-driven value chain. In the banking,[630] health-care,[631] automotive,[632] and even agricultural sectors,[633] a great many decisions and processes are driven by data mining and influenced by AI. These trends unavoidably lead to less transparency and more information asymmetries. Algorithms often act as black boxes, not allowing for data subjects' supervision, understanding, or any other aspect of control.[634] Worse still, deficiencies in the quality and

---

[627] See Chapter 2, section 2.4.2.4.

[628] Information asymmetries between the companies, regulators and consumers came to light during the hearing of Mark Zuckerberg in the US Congress on April 10, 2018, where some of the congressmen revealed fundamental flaws in their understanding of the data economy. Transcript of the hearing of Mark Zuckerberg in the US Congress on April 10, 2018 <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.013eea956ff1> accessed 28 May 2018.

[629] Sophie van Bijsterveld, 'A Crucial Link in Shaping the New Social Contract between the Citizen and the EU' in PJ Stolk and others (eds), *Transparency in Europe II: Public Access to Documents in the EU and its Member States* (Ministry of the Interior and Kingdom Relations Constitutional 2004) 65. The Facebook/Cambridge Analytica scandal is a telling example why transparency is important to guaranteeing legitimate governance of private sector entities. If the Guardian had not revealed Facebook's failure to stop unauthorized data mining, no one would have known about political manipulation on Facebook preceding the US elections and Brexit campaigns. In the future, Facebook plans to label political ads as "sponsored" to enhance transparency of the posters. Carole Cadwalladr and Emma Graham-Harrison, 'How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool' *The Guardian* (17 March 2018) <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm> accessed 5 June 2018.

[630] For example, to early detect credit card fraudulent activity.

[631] For example, to conduct graphical analysis and comparison of symptoms.

[632] For example, to analyse drivers' patterns to improve the technology.

[633] Liliya Pullmann and others, 'WP3 Test of the Model; D3.2 Test Report (Deliverable for the EuDEco H2020 Project)' (2017) <http://data-reuse.eu/wp-content/uploads/2017/09/Test-report-final.pdf> accessed 5 June 2018.

[634] COMPASS, a tool to predict the probability of recidivism used in US courts, was deemed fair by its manufacturer (Northpointe) according to one metric, but found unfair in a later study by ProPublica according to another metric: *'… in the end the decision which notion of fairness to implement is highly political, especially if the decision making system is applied in societally sensitive contexts. Society needs to be made aware of this more.'* Jaap-Henk Hoepman, *'Summary of the CPDP panel on algorithmic transparency' (Blog XOT,* 26 January 2017) <https://blog.xot.nl/2017/01/26/summary-of-the-cpdp-panel-on-algorithmic-transparency/> accessed 5 June 2018.

quantity of the data available to train and test them may lead to discrimination and biases that are always hidden from the public eye.[635]

For these reasons, the need for transparency remains pressing in the data-driven economy. Achieving 'transparent processing', however, is not an easy task and requires more than just information disclosure.[636] In the big data context in particular, providing information must be done *fairly*, that is with particular consideration for an individual's needs. The fact that an individual is probably the weakest link in the data economy draws an important analogy to consumer regulations. In fact, it has been argued that the fairness test in the unfair terms directive[637] could be used to give substance to the notion of fairness in the GDPR.[638] Specifically, fairness could be assessed based on two components: 'good faith' of the data controller and 'significant imbalance' between the controller and the data subject.

5.3. Regulatory framework under the GDPR

5.3.1. The content of the communicated information

5.3.1.1. The information catalogue

Articles 13 and 14 of the GDPR represent the core of the right to information. These two provisions provide a detailed catalogue of the facts to be communicated to a data subject as part of her right to information. The binary nature of the provisions suggests that two types of situations must be distinguished: 1) when data is obtained directly from the data subject, and 2) when data is obtained from third parties.

A typical example of the first situation is the collection of information from a user of a social media network. The moment he signs up for the service and his personal data is about to be processed, the data controller must provide this user with the set of information listed in Article 13.[639] To illustrate the second situation, we can think of a hiring manager within a large enterprise who tries to identify suitable candidates by using information available on social media. Also in this second case, candidates have to be informed about data processing – for example in the job ad.[640] When data is not obtained

[635] Solon Barocas and Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 California law review 671, 693.
[636] A strong link is established in Recital 60 of the GDPR: "*The principle of transparency requires […] any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.*" Section 5.3.2. analysed the exact meaning of that phrase.
[637] *Supra* n 499.
[638] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness Data Protection and the Role of Fairness' [2017] CiTiP Working Paper Series 33-34. Also see Helberger, Borgesius and Reyna (2017).
[639] According to that article, data subjects should at the minimum receive the information about the identity and the contact details of the controller and, where applicable, of the controller's representative, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the legitimate interests pursued by the controller or by a third party (if this is the legal basis used by the controller), the recipients or categories of recipients of the personal data and where applicable, the fact that the controller intends to transfer personal data to a third country or international organization.
[640] Article 29 Working Party, 'Opinion 2/2017 on Data Processing at Work' (2017) 11.

directly from a data subject, two entities may be held responsible for ensuring the information arrives to the addressees, since they are both controllers of data.[641]

The scope of information that has to be provided to data subjects slightly varies between the two situations. Most apparently, it is only when data is not collected from a data subject that there is an obligation to describe categories of data, e.g. address, gender, behavioural data (Article 14(1)(d)). This is probably because in such cases, the data subject does not have a good overview of/control over the data that is being shared. Describing categories helps her understand the nature and scope of data processing, which might otherwise remain hidden. Furthermore, when data **is not** collected from a data subject but is instead gathered from other sources, a data controller has to provide information about *these sources of data* and, if applicable, whether the data came from publicly accessible sources (Article 14(2)(f)).

The information that provision of data is a *statutory or contractual requirement* is only necessary in situations when data is collected directly from a data subject. This is because a data subject has to know about the reasons behind the request for data: is the request just the commercial strategy of a data controller or are there other reasons behind it? Naturally, the situation fundamentally changes if a *law* requires one to disclose personal information. Moreover, a description of a controller's *legitimate interest*[642] should be part of the standard information catalogue when data is collected from the data subject but not when it is collected from third parties, unless necessary for transparency and fairness of data processing. It is difficult to understand why information about legitimate interests of data controllers is less relevant when data is not obtained from an individual.

It is interesting to note that the original proposal of the GDPR drafted by the Commission did not distinguish between the two situations as Articles 13 and 14 in the current version do. Instead, it combined them in one single article. While there were still some differences depending on whether data was obtained from an individual or not,[643] the idea behind the integrated provision was that the two situations were comparable and that the information duty should be considered holistically. However, in the final version of the GDPR, the idea of a uniform article on the right to information was struck down and the Council returned to the old dichotomy system, as it existed in the DPD. As indicated above, the reasons for differentiating the two situations are not very persuasive. Instead of distinguishing between the situations based on a data subject's contact with a controller, the concern should be the context in which the information is obtained.

---

[641] This is the solution that was mentioned in AG Cruz Villalón's opinion to Bara judgement (C-201/14 *Bara and Others* [2015] ECLI:EU:C:2015:638), para. 39.

[642] Recitals 47-50 of the GDPR give some examples of legitimate interests: processing for direct marketing purposes or preventing fraud, transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data, processing for the purposes of ensuring network and information security and reporting possible criminal acts or threats to public security to a competent authority. In *Rigas*, the CJEU provides a three-step tests to assess legitimate interest – *"first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence."* Case C-13/16 *Rigas* [2017] ECLI:EU:C:2017:336, para 28.

[643] See for more details Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 1 final.

The GDPR's information catalogue is extensive; this has two consequences. On the one hand, extensive communications impose a burden on individuals who have to digest long and perplexing policies.[644] On the other hand, data subjects gain access to thorough and detailed information. This may be of special importance in the context of the data-driven economy, where people usually have a greatly limited understanding of what actually happens with their data. Five pieces in the GDPR information catalogue are of particular interest as they either carry special significance for individuals' protection in the era of big data or they are novel. By 'carrying special significance', it is meant that the provisions aim to address specifics of the big data economy, for instance frequent changes of the context in which data is processed and the increased use of automated decision-making. The selected elements relate to information about legal bases for personal data processing, storage of personal data, recipients of personal data and third parties, and personal data processing for new (other) purposes. The provisions in Articles 13(2)f and 14(2)g on the information about automated decision-making merit special attention and are analysed in more detail in section 5.3.1.2.

5.3.1.1.1. Information about legal bases

Contrary to the DPD, which did not address this point, the GDPR places emphasis on ensuring that data subjects are aware of the legal basis used to justify the data processing. In the GDPR, conveying the information about legal bases is a mandatory provision (Articles 13(1)(c) and 14(1)(c)). Data controllers are obliged to inform data subjects about any legal bases that they use, for example data subjects' consent, public interest, or a contract between the controller and data subject. If data processing is based on a legitimate interest of a data controller, these interests also have to be elaborated and communicated to a data subject (Articles 13(1)(d) and 14(2)(b)). By receiving the information on legitimate interests, data subjects become more aware of controllers' intentions and can more easily assess what is happening with their data.

The information on the basis of Articles 13(1)(c) and 14(1)(c) should also reflect the results of the balancing test, which controllers are obliged to carry out whenever legitimate interest is used as a basis of data processing. It should be demonstrated that controllers have carefully balanced their commercial interests with the fundamental rights and interests of data subjects, ensuring that their fundamental rights protection is not at risk.[645] This is important because in the case of secondary data uses, controllers are often pursuing solely commercial interests. In such cases, controllers may find it difficult to justify *'in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.'*[646] It is most

[644] Suzanne Rodway, 'Just How Fair Will Processing Notices Need to Be under the GDPR?' (2016) 16 Data Protection - A Practical Guide to UK and EU Law. Also see sections 2.4.2.2. and 4.2.3.

[645] Article 29 Working Party uses the example of pizza order to illustrate when processing cannot be based on legitimate interest. In the example, Claudia orders a pizza via a mobile app on her smartphone, but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home. Claudia's address and credit card details but also her recent order history (for the past three years) are stored by the pizza chain. In addition, the purchase history is combined with data from the supermarket where Claudia does her shopping online, which is operated by the same company as the one running the pizza chain. Article 29 Working part considers that in such a case a company could not base data processing on their legitimate interests (i.e. pizza delivery and charging for the costs) because they too strongly interfered with Claudia's rights (i.e. collected too much of her personal data). Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' 31.

[646] Ibid., 43.

likely in such cases that the interests of data subjects will prevail over controllers' commercial interests.[647]

The provisions in Articles 13(1)(c) and 14(1)(c) face two challenges. First, they are difficult to implement because they both require a highly specific description of the interests and careful balancing with the rights of individuals. To justify that/why their interests override the rights of data subjects, controllers have to carefully identify and specify these interests in the first place. Furthermore, coming up with a balancing scheme may impose some additional administrative burden.[648] Second, the provisions may be used as a *carte blanche* in a wide range of cases. To avoid generalisation, the balancing test under legitimate interest requires a context-specific assessment and implementation of potential mitigations as part of organisational accountability.[649]

5.3.1.1.2. Information about the length of the storage period

As a new part of the information catalogue, the GDPR obliges data controllers to provide information about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Articles 13(2)(a) and 14(2)(a)). This 'new' category is in line with the principle of storage limitation, which is expressly laid down in the GDPR.[650]

In the data-driven economy, local data storage on external hard drives has almost disappeared. Due to the possibility of limiting cost, companies are increasingly using cloud storage solutions. This has at least two consequences. First, the cost of data storage has decreased; a larger amount of data can be stored for a longer period of time. Second, this new type of data storage typically requires the involvement of a third party in the data processing. Dropbox and Amazon Web Services are two widely known cloud providers commonly used by businesses.

The processing of personal data should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.[651] In particular, this requires ensuring that the period for which the personal data are stored is limited to a strict minimum.[652] This in turn decreases the risk of wrongful or extensive uses, as less data is exposed to potential abuses for a shorter time period. This requirement bears special value given that illegitimate retention of personal information has been among the most significantly contested online information practices.[653] For example, a cloud-based storage provider does not let users' data lie dormant on the servers but often shares or sells it to third parties. Dropbox's privacy policy informs users that the company will not sell their data to advertisers or other third parties.[654] However, it also provides a long list of exceptions, such as government, other

[647] Santos and others, 26.
[648] For an example of such scheme see Centre for Information Policy Leadership (2017), 18. This report gives a surprisingly positive assessment of the possibility to rely more often on legitimate interest as a basis for data processing.
[649] E.g., pseudonymisation of data. Ibid., 29.
[650] Article 5(1)e of the GDPR.
[651] Ibid.
[652] Recital 39 of the GDPR
[653] Joel Reidenberg and others, 'Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding' (2015) 30 Berkeley Technology Law Journal 56. Also in relation to concerns of excessive data retention see Alexander Tsesis, 'The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data' (2014) 49 Wake Forest Law Review 433 <http://wakeforestlawreview.com>.
[654] Dropbox's privacy policy <https://www.dropbox.com/privacy> accessed 5 June 2018.

users, trusted parties, and other applications.[655] Having the information about data controllers' storage policy also raises awareness of potential data reuses and helps assess their risk.

5.3.1.1.3. Information about third parties and recipients of data

As was shown in Chapter 2, data disclosures and sharing (aimed at combining and reusing third parties' data sources) have become an inherent part of the modern data economy. The negative side of this is that individuals are often unaware of flows and secondary uses of data which do not meet their privacy expectations.[656] The requirement in Articles 14(1)(e) and 13(1)(e) seems to have acknowledged this struggle. The articles require that controllers provide information about recipients or categories of recipients of personal data.[657] However, the provision is far from the ideal situation depicted in an earlier opinion by the Article 29 Working Party. Namely, the Working Party suggested that when data was collected online, the websites (i.e., controllers) should provide information not only about to whom personal data would be disclosed, but also about *why*.[658] This is not expressly stipulated in the GDPR.

A 'recipient' stands for a natural or legal person, public authority, agency, or other body to which the personal data is disclosed, whether a third party or not. However, the GDPR stipulates that public authorities, which may receive personal data in the framework of a particular inquiry in accordance with EU or member state law, shall not be regarded as recipients (Article 4(9) of the GDPR). This means that the fact that users' data has been shared with public authorities should not be provided under the right to information.

Does this also mean that informing data subjects that their data has been shared with public authorities in the sense of a 'canary clause' is not provisioned/allowed? A canary clause is a statement on a website declaring that the service provider has not received any secret data snooping requests from the government or law enforcement agencies. After such a request has been made, the notice is removed from the website.[659]

It is clear that sometimes protection of public interest and security require absolute confidentiality.[660] However, more transparency over data flows between the government and private data holders seems to be increasingly needed. These flows are ubiquitous, but they are often completely hidden. This issue was also challenged in the PNR case, where the CJEU stressed the importance of transparency regarding data flows to government agencies.[661]

---

[655] Ibid.

[656] See for example the transcript of the hearing of Mark Zuckerberg in the US Congress on April 10, 2018 <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.013eea956ff1> accessed 28 May 2018. Even some of the US Congressmen and Congresswomen were clearly unaware of Facebook's business model and the use of data on the platform.

[657] Differently from the directive, under which this information was only exceptionally provided as part of "further information". See Article 10(c) of the DPD.

[658] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) 31.

[659] 'What is a warrant canary?' *BBC* (5 April 2016) <http://www.bbc.com/news/technology-35969735> accessed 5 June 2018.

[660] See article 23(1) which lists exceptions to data subject rights.

[661] Opinion 1/15 of the Court regarding Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data [2017] ECLI:EU:C:2017:592, para 223.

Interestingly, the EU Parliament's (LIBE) proposal for the GDPR contained a requirement to inform a data subject '*whether personal data was provided to public authorities during the last consecutive 12-month period*'.[662] The provision was later removed from the information requirement.[663] This removal does not suggest that a canary clause or some general information on data sharing with the government should not be presented to data subjects at all. On the contrary, a general clause can be a helpful tool to achieve more transparency about data flows (while not jeopardising ongoing investigations).[664]

The provision requiring that information about recipients always be provided to data subjects is of course a welcome improvement. It is, however, limited by the scope of the GDPR. For instance, once data is anonymised, data protection law in principle ceases to apply.[665] In the case of anonymised data sharing, recipients do not have to be disclosed.[666]

5.3.1.1.4. Information about new (other) purposes of data processing

Where a controller intends to further process personal data for a purpose other than that for which it was collected, prior to that further processing the controller shall provide the data subject with information on that other purpose and any further relevant information (Articles 13(3) and 14(4)).[667]

In practical terms, this obligation means that if the controller later processes personal data for a new purpose not covered by the initial notice, then it must provide an updated notice covering this new processing.[668] This requirement did not exist in the DPD. It is yet another reflection of the changes that have taken place in the global economy in recent years and to which the legislator paid special attention. Data reuse and sharing have been two of the key business strategies of data-driven companies. A typical example is social media platforms: data collected by users is traded to third parties, e.g. advertisers or data brokers, to be reused for their specific purposes.[669] Furthermore, predictive analysis may transform information about someone's shopping habits into information on someone's health status (e.g. pregnancy). In the well-known Target case, a store learned that a

---

[662] European Parliament, 'European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))' Committee on Civil Liberties, Justice and Home Affairs (LIBE)(2013) Amendment 110 <http://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-4492192886392847893.pdf> accessed 5 June 2018.

[663] The reasons are unknown. My assumption is that the security objectives prevailed over the need for transparency.

[664] Some data controllers already provide such information, see for example Facebook's privacy policy and their transparency report <https://transparency.facebook.com/government-data-requests> accessed 5 June 2018.

[665] However, this depends on the strength of anonymisation. It is possible that anonymised data is de-identified. Then data protection law would apply again. See for example Tene and Polonetsky (2013) 257.

[666] The case of Unroll, a free inbox cleaning software, well illustrates issues at stake. ' *... while Unroll.me is cleaning up users' inboxes, it's also rifling through their trash. When Slice found digital ride receipts from Lyft in some users' accounts, it sold the data off to Lyft's ride-hailing rival, Uber.'* Amanda Hess, 'How Privacy Became a Commodity for the Rich and Powerful' *The New York Times* (May 9, 2017) <https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html> accessed 5 June 2018.

[667] Article 13 (3) of the GDPR.

[668] Bird & Bird (2017) 21.

[669] The lack of vocabulary complicates the definition of the phenomenon of 'online personal data trading'. Advertisers pay to social networks to place relevant ads. The ads are allocated to a user based their profiles. Although, formally speaking, the advertisers *pay for a service* to Facebook, what actually happens is a sale of consumers' data. However, the social media executives vehemently refuse to frame this as 'selling of data'. See for instance the exchange between Mark Zuckerberg and senators at the hearing in US Congress on April 10, 2018, *supra* n 628.

teenager was pregnant before her father did. Based on the teenager's shopping profile, which was comparable to that of pregnant women in its database, the retail store predicted that she was expecting a baby and started sending advertisements for maternity products. This became a huge scandal after the teenager's father (and not the teenager herself) received the ads. The story clearly demonstrates the unexpected and out-of-context insights that predictive analysis may have.

Changes to the purpose of data processing often happen as part of a business routine. Recruiters use social media data to pre-screen suitable candidates. This challenges the privacy expectations of social media users. Most people who share personal data on social media expect it to be processed for the purpose of enabling online communication and find it surprising when this data is processed as part of a recruitment strategy. Without receiving specific, preliminary information about intended purposes, it is extremely difficult for any individual to ascertain to which uses specific data is actually being put.[670] Conveying information about the purposes is even more important as data reuse is increasingly carried out behind the scenes.

As mentioned in the overview of the EU data protection law in Chapter 3, purpose limitation is one of the core restrictions in this law. Under the principle of purpose limitation, data cannot be reused unless the controller ensures a valid legal basis for this secondary use, e.g. a data subject's additional consent. This is of course at odds with the big data business practices, which tend to make a profit from data secondary uses. Furthermore, the process might become lengthy and inefficient if each time a data controller uses the data for a new purpose, this has to be communicated to data subjects. Yet, the GDPR remains strict in this regard, as do some EU data protection authorities. In a letter to Microsoft regarding its Windows 10 privacy policy, the Article 29 Working Party expressed concerns about the scope of data being collected and further processed.[671] Microsoft processed data collected through Windows 10 for different purposes, including personalised advertising. It appears from the letter that this general description was not enough for the EU watchdog: '*Microsoft should clearly explain what kinds of personal data are processed for what purposes*,' the Working Party wrote, demanding Microsoft's immediate reaction.[672] Moreover, a recent document of the Dutch DPA confirms that authorities are dedicated to keeping the principle intact. The DPA found that Facebook acted in breach of data protection law as the company did not adequately inform data subjects that *'it can track web surfing behavior and app usage outside of Facebook and use these data for advertising purposes.'*[673] This sort of tracking may easily cross the boundaries of purpose limitation, but it is difficult to notice

[670] In a 2015 report, KU Leuven researchers point at Facebook's DUP which only provides a broad overview of the purposes for which it processes personal data. '*This overview, however, is extremely generic and encompasses all data collected by Faceboo*k.' Alsenoy and others (2015) 66.

[671] Letter of the Working Party 29 to Microsoft from 12 January 2016 <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwi5tPrJoJPVAhVB9IMKHeg0Bv8QFggoMAA&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D42572&usg=AFQjCNHHyjIqeD5bRZFDbiXGX2rEwlfVQA> accessed 5 June 2018.

[672] Ibid.

[673] Informal English translation of the conclusions of the Dutch Data Protection Authority in its final report of findings about its investigation into the processing of personal data by the Facebook group from 23 February 2017 <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_facebook_february_23_2017.pdf> accessed 5 June 2018.

and escape from. Direct information – the Dutch DPA stressed the need to provide information in the first layer of the privacy notice – is therefore of paramount importance.[674]

5.3.1.1.5. Information about the sources of data

When data is obtained from third parties, controllers have an additional duty to provide information about those third-party sources and, if applicable, whether the data came from publicly accessible sources (Article 14(2)(f)). This is another novel provision in the GDPR that also seems to fit new circumstances in the data-driven economy, where data collection is rarely limited to one source.

For example, consider the new trend in the pharmaceutical industry: real world data (RWD). RWD is used to improve clinical trials with data collected from sources outside the traditional clinical environment. These sources may include large simple trials, pragmatic clinical trials, prospective observational or registry studies, retrospective database studies, case reports, administrative and health-care claims, electronic health records, data obtained as part of a public health investigation or routine public health surveillance, and registries (e.g., device, procedural, or disease registries).[675] The unique combination of sources can contribute to better results of clinical trials and enable more precise analysis of drugs' effects. However, by connecting different sources, it is easy to reveal facts about a person and infringe her privacy. A combination of someone's social media profile and her clinical trial report can be much more insightful and, for precisely these reasons, privacy-infringing. Combining data sources is also a trend on some other data-driven markets. Facebook has admitted to regularly combining and enriching its own data with databases purchased from Acxiom.[676] Merging someone's social media profile data with information about his health or race can be a valuable source of information for advertising companies – those that are Facebook's most loyal clients.[677] In a recent opinion, the Dutch DPA pointed to the lack of transparency in relation to Facebook's data sources, which also added to the violation of its information duty: '*The Facebook group does not offer a central overview of the personal data it processes for advertising purposes since the change of the privacy policy. The information is scattered over different sources. Because of this, data subjects do not receive a clear and understandable overview of the data processing with the highest impact on their private life in the first information layer.'*

The two examples above illustrate why knowing about sources is critical to be aware of the scope of data processing. However, the GDPR's rule to disclose sources has been watered down by the guidelines in Recital 61. Namely, if the origin of the personal data cannot be provided to the data subject because various sources have been used, the recital suggests that only general information

---

[674] *'The Facebook group is able to do this as soon as a Facebook user visits a website or uses an app that contains a Facebook 'like' button, or other interaction with Facebook, even if the user does not click on that button, and even if the user has been logged-out of the service.'* Ibid.

[675] Food and Drug Administration, 'Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices - Guidance for Industry and Food and Drug Administration Staff Document' (31 August 2017) <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm513027.pdf> accessed 23 September 2018.

[676] Only recently, under the media and public pressure, they abandoned this practice. Drew Harwell, 'Facebook, longtime friend of data brokers becomes their stiffest competition' *The Washington Post* (29 March 2018).

[677] Jim Edwards, 'Facebook's Big Data Partner Knows Who You Are Even When You Use A Different Name On The Web' *Business Insider* (September 26, 2013) <http://www.businessinsider.com/facebook-and-acxioms-big-data-partnership-2013-9> accessed 5 June 2018.

should be provided. This provision appeared in the GDPR text after the Council's intervention and allows for a wide interpretation of how far information duty under Article 14(1)(f) actually extends.[678]

In the technical terminology, the discussion on data sources has been framed as data lineage or provenance: a description of where data came from, how it was derived, and how it is updated over time.[679] One important reason to be interested in data lineage is to find sources of errors. Thus, controlling the truthfulness of the data is at the heart of data lineage. The GDPR requirements on data sources convey a similar idea. By transparently presenting the sources, it is more likely to control data's adequate use and outcomes of its analysis.

5.3.1.2. The right to explanation

5.3.1.2.1. Information about automated decision-making in Articles 13 and 14

Another highlight in Articles 13 and 14 is the right to receive information about automated decision-making. At least when data controllers engage in automated decision-making, including profiling, which is based solely on automated processing and which produces legal effects concerning a data subject or similarly significantly affects a data subject,[680] data subjects must be provided with meaningful information about the logic involved in the decision-making and about its significance and envisaged consequences (Articles 13(2)f and 14(2)g).

In the DPD, information about the logic behind automated decisions was only provided if a data subject herself demanded so through her right of access (Article 12a of the DPD). The GDPR has preserved this provision but also includes information on automated decision-making in the standard information catalogue.

This new information duty has sometimes been referred to as a right to *explanation*, suggesting that it could work as a right to clarification of complex algorithms and decisions inferred from them.[681] In the context of the data-driven economy, the right to explanation could indeed play an important role. Data-driven decisions are often hidden from the public eye, are based on complex algorithms that are difficult to comprehend, and have consequences that cannot easily be predicted.[682] Explanation tailored to the needs of data subjects thus appears to be desirable.

The duty to provide information on automated decisions is not limited to the cases where the decisions produce legal effects; these are only the cases where informing data subjects is *mandatory*. However, given the risks of automated decision-making, it could be argued that the right should have a broader scope. Automated decision-making, in particular profiling, often lead to discrimination and causes

---

[678] Materials from the GDPR negotiations in the Council <http://data.consilium.europa.eu/doc/document/ST-9281-2015-INIT/en/pdf> accessed 5 June 2018.

[679] Leonardo Haut, Marius Brinkmann and Sven Abels, 'WP2 Developing the Initial Model: D2 .4 Report on the Technological Analysis (Deliverable for the Eudeco H2020 Project)' (2016) 7 <http://data-reuse.eu/wp-content/uploads/2016/06/D2.4_ReportOnTheTechnologicalAnalysis-v1_2016-02-29.pdf> accessed 5 June 2018.

[680] As for the specific definition of these automated decisions Articles 13 and 14 refer to Article 22 of the GDPR.

[681] Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and A "right to Explanation"' <http://arxiv.org/abs/1606.08813> accessed 5 June 2018; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2018) 7 International Data Privacy Law 233.

[682] Illustrative is the example of the teachers' ratings used in the US, where the parameters which a teacher is judged upon, are largely unknown. See more in Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016).

biases due to deficiencies in the quality and quantity of the data available to train and test the algorithm, as well as problems with data sources and labelling.[683] The risk for fairness is thus inherently present,[684] which is an argument for why information on automated decision-making should almost always be provided to a data subject.

What specifically should information on automated decision-making entail? Based on Articles 13(2)f and 14(2)g, data subjects should receive the following three subcategories of information:

1. Meaningful information about the logic involved in the automated decision-making;
2. Meaningful information about the significance of the processing;
3. Meaningful information about the envisaged consequences of the processing.

Logic stands for the types of data and features considered in an automated decision-making system, and categories in the decision trees used to make a decision.[685] Linear models, which can only represent simple relationships, are typically easy to explain, whereas nonparametric methods such as support vector machines and Gaussian processes, which can represent a rich class of functions, are often highly difficult to interpret.[686] For example, data mining software performing on the basis of multiple variables (even thousands) can lead to a process that is not explainable in human language.[687] It would be difficult for the user of the software to provide a detailed answer to why an individual was singled out to receive differentiated treatment by an automated recommendation system. This is why some have argued that '*algorithmic approaches are alone in the spectrum in their lack of interpretability*'.[688]

Edwards and Veale examined the computer science literature to determine what it means to explain an algorithm in a meaningful way.[689] They identified two types of explanation: subject- and system-centric. The former, which is restricted to the region surrounding a set of data, was suggested as more meaningful, mostly because it enables users 'to build more effective and relevant mental models'.[690] Other solutions that could help convey the logic of the systems to individuals without going into technical details are the use of counterfactuals, simple 'if-then' statements indicating which external facts could be different to arrive at a desired outcome,[691] and case-based approaches that provide explanation by retrieving the most similar cases from computer memory.[692] Finally, a useful explanation of the logic that is used to arrive at the decision should also include an explanation of the type of data on which the decision is based.[693]

---

[683] Dimitra Kamarinou and others, 'Machine Learning with Personal Data Machine Learning with Personal Data' [2016] Queen Mary School of Law Legal Studies Research Paper No. 247/2016.
[684] Among others, power imbalance and violations of the principle of good faith.
[685] Wachter, Mittelstadt and Floridi (2017) 6.
[686] Goodman and Flaxman (2016) 6.
[687] Andrejevic and Gates (2014) 186.
[688] PJG Lisboa, 'Interpretability in Machine Learning – Principles and Practice' in Francesco Masulli, Gabriella Pasi and Ronald Yager (eds), *Fuzzy Logic and Applications. WILF 2013.* (Springer International Publishing 2013).
[689] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for' (2017) 16 Duke Law and Technology Review. See also a related discussion in Section 5.4. of this thesis.
[690] Ibid.
[691] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 2.
[692] Dónal Doyle, Alexey Tsymbal, Pádraig Cunningham, 'A Review of Explanation and Explanation in CaseBased Reasoning' <https://scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-41.pdf> accessed 27 December 2018.
[693] Edwards and Veale (2017); Wachter, Mittelstadt and Floridi (2017).

The second subcategory, the *significance* of the decision, has two connotations: the objective and the subjective one. The *subjective* significance refers to an individual's own perception of the effect(s) of the automated decisions.[694] In the face of an increasingly automated and inhuman(e) data-driven world,[695] such subjective considerations should certainly be taken into account. For example, showing an appropriate ad that upsets someone could be subjectively significant. A drastic example comes from the US, where a woman was being shown advertisements for burial urns six months after her mother passed away.[696] The *objective* significance is established when a decision is regarded by a considerable number of other persons as significant.[697] For example, an automatic assessment of a financial situation by a bank may be viewed as banal by wealthy persons, but it may represent a significant decision for the people who financially depend on access to the bank loan.

Finally, *envisaged consequences* of automated decision-making relate to consequences that can be conceived as a possibility due to data processing.[698] In principle, these consequences refer to the opportunities and risks that individuals gain/take by sharing their data.[699] Risks are of particular relevance since in principle controllers tend to disregard them. Hildebrandt believes that the provision should be interpreted broadly.[700] In her view, the effects that are not intended but can be envisaged due to the generative nature of profiling must also be accessed and communicated.[701] Recently, social media networks have become a key source of information for recruiters. For two thirds of recruiters, LinkedIn is the most important social network for candidate sourcing.[702] Recruiters are able to employ LinkedIn's own search tools to select candidates to invite to a job interview. Putting this example into perspective, the social networks should provide users with information about the automated decision-making and about the risk of not being considered for a job. In this regard, Hildebrandt points out the important link between this requirement and the principle of purpose specification: *'the purpose specification principle is reinstated as an important legal rule, because envisaging effects requires ex ante specification of the targeted effects.'* [703]

Under Articles 13 and 14, the GDPR seems to guarantee an *ex ante* explanation but it does not include the explanation of a specific, individual decision that would be provided *ex post* data processing.[704] This drawback could be mitigated with some other provisions of the GDPR, for example the right to access

---

[694] Lee A Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Report 25.
[695] Inhumane here refers to both – consisting of artificial intelligence and lacking respect for human dignity.
[696] Rosiebita (@Rosiebita), 'Had the same situation with my mother's burial urn. For months after her death, I got messages from Amazon saying, "If you liked THAT urn, you might also like THIS one!"' (6 April 2018) <https://twitter.com/rosiebita/status/982293240261914625> accessed 16 June 2018.
[697] Bygrave (2001) 8. Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855> accessed 14 June 2018..
[698] 'envisage', Oxford Living Online Dictionary <https://en.oxforddictionaries.com/definition/envisage> accessed 14 June 2018.
[699] Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in Jacques Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press 2012) 51.
[700] Ibid.
[701] Ibid.
[702] Right management <http://www.kent.ac.uk/careers/jobs/social-networking.htm> accessed 5 June 2018.
[703] Hildebrandt (2012) 51.
[704] Wachter, Mittelstadt and Floridi (2017) point out the inappropriate use of the phrase – right to explanation. Namely, the right to have a decision explained is not provided anywhere in the binding GDPR text. There is a short reference in Recital 71, however this is not a binding text and the legislative history documents indicate that the legislator deliberately decided not to include it in the binding part.
[704] Wachter, Mittelstadt and Floridi (2017) 1.

in Article 15 and the right to contest the decision in Article 22.[705] Nevertheless, the new right to information on automated decision-making is a bright point in the GDPR. First of all, the provision has become a constituent part of the 'information catalogue', which increases the likelihood that data subjects will come across it. Second, if interpreted favourably, it could help establish a system of more accountable and transparent data processing by data controllers.

5.3.2. The quality of communication

Article 12 of the GDPR stipulates requirements in relation to transparency and modalities to facilitate individual rights. Paragraph 1 describes some distinct attributes of the communicated information by requiring that data controllers provide it '*in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'* In comparison to the DPD, this GDPR provision expressly requires data controllers to adopt a more transparent, user-friendly, and open approach.

Two sorts of requirements stem from the first paragraph of Article 12. The first relates to the quality of the form in which information is provided. This has to be concise, transparent, intelligible, and easily accessible. The second relates to the language, which has to be clear and plain.[706]

Concise means that information is given clearly and in a few words: brief but comprehensive.[707] Concise writing conveys the writer's points succinctly, without superfluous words, and with an appropriate level of detail.[708] The final result is that the text is clearer and more engaging for the reader.[709] For example, after being subject to a thorough review by the European data protection authorities, Google's privacy policy has been extended, however information is no longer provided in one single passage but structured in several paragraphs and bullet points to ease reading.[710] By using this layered format, it has become more concise.

A related requirement is intelligibility; *intelligible* stands for something that can be understood or comprehended. If 'concise' refers to the information itself, being intelligible necessarily involves a data subject. To be comprehended and understood, information has to be presented in a way that is suitable to the intellectual capabilities of a data subject. The bar should not be set high. In fact, it has been shown that the intelligibility for data subjects in the online environment has been highly limited.[711]

In principle, intelligibility has to be assessed according to the abilities of an ordinary person. However, fulfilling the right to (access to) *quality* information will sometimes require that we consider in what

---

[705] Edwards and Veale (2017) 35.

[706] In English, use of actives verbs, omission of legal jargon and sticking to the commonly used structure has been suggested as the optimal one. In other languages, a similar simplistic approach should be considered. Language properties also face challenges. One of them is use of English, which is a *lingua franca* of the Internet. Many data subjects are not native speakers of English, which means that they are more likely to run into some comprehension difficulties. Because of the internet jargon, language is a problem also for natives.

[707] 'concise' Merriam-Webster Online Dictionary <https://www.merriam-webster.com/dictionary/concise> accessed 4 June 2018.

[708] Mark Osbeck, 'What is "Good Legal Writing" and Why Does It Matter?' (2012) 4 Drexel Law Review 417, 438.

[709] Ibid.

[710] Lisa Mazzie Hatlen, 'Conciseness in Legal Writing' [2009] Wisconsin Lawyer, the official publication of the State Bar of Wisconsin. Also, conciseness is closely linked to the requirement to use clear and plain language.

[711] Among the reasons is technological complexity due to particular nature of data, information overload that complicates communication, and individuals' psychological limitations such as bounded rationality. See more in section 4.5.

format the information will be most comprehensible to one particular group of people. The following are two distinct situations in which the proper way of providing information plays a significant role:

a) where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom, and for what purpose personal data relating to him is being collected, such as in the case of online advertising;
b) where processing is addressed to a child (Recital 58).[712]

The complexity described under a) is an inherent part of the data-driven economy. For example, explaining algorithmic decision-making requires a different level of detail and simplification than providing contact information of a data protection officer.[713]

Easily accessible refers to the channels through which the information is retrieved. In the context of online privacy, it relates to the architecture of the website or electronic devices through which the information is provided. Article 12 stipulates that when appropriate, information should be provided in electronic form. One example of such a provision of information is through a website (Recital 58). Another option is access through a mobile app. Apps present a technology that can work to the advantage or disadvantage of a user who wants to be informed. On the one hand, app developers are often in the best position to provide notice and disclosure due to the proximity to the end-user.[714] On the other hand, lack of knowledge about privacy rules, limitations inherent in current mobile architecture, and dependence on third parties may undermine these good prospects.[715] The Article 29 Working Party has expressed fear that apps could disguise information important for a user: '[It] … *is unacceptable that the users be placed in a position where they would have to search the web for information on the app data processing policies instead of being informed directly by the app developer or other data controller*.'[716] For efficiency purposes, controllers should ensure that data subjects are aware of the decision-making system concerning them. This would not only benefit individuals but also public authorities, which could more easily assess the legality and ethics of an algorithm and the process through which a decision has been made. Indeed, a system that is not auditable is a system one should not use.[717] Hence, access to (understandable) information is as important as the information itself.[718]

---

[712] As regards b) the GDPR's Recital 58 makes a distinction between information that is provided to an adult and the information that is provided to a child. The latter should contain clear and plain language that the child can easily understand.
[713] Article 13(1)(b) of the GDPR.
[714] Future of Privacy Forum and The Center for Democracy & Technology, 'Best Practices for Mobile Application Developers' (2011) 1 <https://fpf.org/wp-content/uploads/Best-Practices-for-Mobile-App-Developers_Final.pdf> accessed 14 June 2018.
[715] Ibid.
[716] Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' [2003] 23.
[717] See Mark Rotenberg's comment at the CPDP 2017 conference quoted by Hoepman, *supra* n 634.
[718] It should be borne in mind that data-driven algorithms can also be transparent and fair, even more than humans. Humans often make very biased decisions, are often not able to reliably 'explain' their decisions and are also hard to de-bias. See Gummadi's comment at the CPDP 2017 conference quoted by Hoepman, *supra* n 634. At the same time, the author also realises that there are many notions of fairness, and that a thorough mathematical formalisation of these notions showed that some notions of fairness are incompatible: they cannot be achieved both at once. A technological understanding of fairness can be different from a traditional legalistic understanding. For a technical understanding of fairness see for example Matt Kusner and others, 'Counterfactual Fairness', *1st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA* (2017).

The final requirement is *transparency*. In the ordinary sense, transparent means that there are no hidden agendas and that all information is available.[719] The dictionary definition in fact comes quite close to Recital 39, which describes transparency as an umbrella term for all other qualities of information listed above.[720]

In the data-driven economy, transparency is a challenging task. Three trends in particular are concerning. First, transparency can be threatened by the fact that data controllers are likely to conceal their methods, such as data mining and data sharing. Data mining details may be protected under intellectual property laws. The GDPR recognises the interest of companies in keeping the information about their internal decision-making processes confidential if disclosure would negatively affect their trade secrets, patents, or copyright-protected assets.[721] The reason for this provision is that forcing companies to reveal algorithms may clash with innovation objectives.[722] In addition, controllers are not explicit about those with whom they share information. In the aftermath of the Facebook and Cambridge Analytica scandal, it became obvious that Facebook users' data was shared with third-party apps on a daily basis – but only few users knew that their information was transferred all around the world.[723]

Second, transparency can be at risk because of the architecture of modern data processing systems, which sometimes do not allow for any meaningful explanation of their functionality. For instance, some types of AI analysis such as machine learning may yield unexpected, novel results that cannot be explained beforehand to data subjects because they develop gradually, learn from past decisions, and therefore become largely unpredictable.[724] For example, AlphaGo, Google's deep mind software, has been learning from its own experience, which makes it extremely difficult to understand its actions and to predict how the algorithm will behave in the future. During the latest battle between AlphaGo and a Chinese master, no one expected that the software could win. Only after AlphaGo's effortless performance did the developers realise how greatly its learning skills had improved and what sorts of decisions it had become capable of.[725]

Finally, transparency 'as a method to see, understand and govern complex systems' may sometimes be misleading or even actively unhelpful.[726] For instance, transparency of certain data mining processes may give an impression that they are sound, while the data that is being mined is in fact flawed and the outcomes unreliable. Because of this, it has been suggested that the focus of transparency in data-

---

[719] 'transparent' *Black's Law Dictionary* (1910).
[720] '*The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.'*
[721] Recital 63 of the GDPR. Here, the GDPR basically anticipates that non-disclosure would typically be required by IP laws anyway.
[722] Katja De Vries, Sari Depreeuw and Mireille Hildebrandt, 'D3.2 Profile Transparency, Trade Secrets and Intellectual Property Rights in OSNs – v1 (Deliverable for the USEMP Project)' (2015) 9.
[723] *Supra* n 628. During the hearing, the congressmen and the Facebook CEO discussed hidden facts related to Facebook's data sharing practice which, after they had become public, received strong disapproval.
[724] JA Kroll and others, 'Accountable Algorithms' [2016] U. Pa. L. Rev. 633, 638.
[725] Sam Byford, 'AlphaGo's battle with Lee Se-dol is something I'll never forget' *The Verge* (15 March 2016) <https://www.theverge.com/2016/3/15/11234816/alphago-vs-lee-sedol-go-game-recap> accessed 5 June 2018.
[726] Lilian Edwards and Michael Veale (2017) 34.

driven processes should not be on understanding the technical process, but on providing information that would enable data subjects to contest a decision[727] and to hold controllers accountable.[728]

While the GDPR's criteria on the quality of information surely suffer from multiple deficiencies, some positive steps forward have been made. In 2014, Custers, van der Hof, and Schermer examined privacy expectations of social media users and identified four criteria for decent privacy policies: 1) Is the information provided specific and sufficiently detailed? 2) Is the information provided understandable? 3) Is the information provided reliable and accurate? and 4) Is the information provided accessible? In the DPD, only criteria 1 and 3 were addressed to some degree. In the GDPR, all four criteria have been implemented.[729]

5.3.3. The form of communicating the information provisions

Regarding the form used to communicate the information to data subjects, the GDPR only provides some minimal hints. *Form* means the organisation, shape, and structure of something.[730] In terms of the shape, the GDPR mentions a few options: the information shall be provided in writing or by other means (e.g. icons, see section 5.3.3.1.1), and when appropriate by electronic means.[731] Given the increasing amount of data that is processed online, the electronic form should be prioritised. One example of the electronic form that the GDPR explicitly mentions is through a website (Recital 58). The alternative is providing information through a mobile app.[732]

With regard to the organisation, the information is typically communicated in one of the following two ways: as a privacy policy, or as part of general terms and conditions.[733] Below, these two means of organising the information function in the context of the data economy and their impact on individuals' control over personal data are assessed in more detail.

5.3.3.1. Privacy policies and/or notices

Privacy policies are internally focused tools that declare a company's policy regarding personal data use and how the company intends to achieve compliance with privacy principles.[734] Today, the majority

---

[727] Wachter, Mittelstadt and Russell (2018).

[728] boyd, danah, "Transparency != Accountability" (2016) EU Parliament Event 07/11 Algorithmic Accountability and Transparency <http://www.danah.org/papers/talks/2016/EUParliament.html> accessed 5 June 2018.

[729] van der Hof, Schermer and Custers (2014).

[730] It should be distinguished from methods. While the GDPR goes into detail of the quality of communication to data subjects (see section 5.3.2.), it does not elaborate on specific *methods* used to convey the required information. *Methods* stand for the procedure, technique, or way of doing something. The regulation maintains an open regime from the DPD, which left the implementation of the requirements up to data controllers. The directive made no distinction between actively communicating information about privacy practices and simply making it readily available to data subjects. Based on the unchanged wording and structure of the provision in the GDPR, this interpretation should uphold. Ustaran and International Association of Privacy Professionals (2012) 115.

[731] Article 12(1). When necessary, information may also be communicated orally, under the condition that the identity of a data subject is known.

[732] See also section 5.3.2. on 'quality of information'.

[733] Eleni Kosta, *Consent in European Data Protection Law* (Nijhoff 2013) 310.

[734] Contrary to privacy policies, privacy notices are externally oriented. If carefully designed, they should support objectives of transparency by alerting individuals as to what is being done with their personal data. Neil Robinson and others, 'Review of the European Data Protection Directive' (2009) <https://www.rand.org/pubs/technical_reports/TR710.html> accessed 6 June 2018. In comparison to privacy policies they are shorter and more concise. Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2012). In practice, the difference between notices and policies is often blurred and both words have been used to describe statements about a company's approach to protection of personal data.

of companies in Europe have a privacy policy.[735,736] While there is no explicit legal duty for a company's website to publish a policy, having one is usually the only practicable method of performing the company's informational duties towards users on the site.[737] This increased transparency was also mandated by industry self-regulation, as companies acknowledged stronger consumer demand for information.[738] Post-GDPR, many data-centered companies have made a noticeable move toward updating the language and format of their privacy policies.[739]

Policies are the main source of information for a data subject, in particular to help her decide whether to consent to data processing or not.[740] However, if consent is not used as a legal basis, this does not render privacy policies superfluous. They can be still important for those data subjects who would like to trigger their rights in relation to personal data, for instance the right of access or the right to object. Having meaningful information therefore plays a role that goes beyond consent.

Not only individuals but also other parties such as policy-makers, academics, researchers, investors, advocates, and journalists benefit from these disclosures.[741] Courts and DPAs tend to examine companies' online policies and/or statements especially closely in terms of whether they provide the necessary information and transparency.[742] European DPAs have demanded changes to Facebook', Tinder's, Google's, and Microsoft's policies.[743] It is important to note that investigation of privacy policies often requires a joint effort by several authorities.[744]

As mentioned, providing information and obtaining consent typically form an indivisible whole. Consent is a highly problematic concept, and this also has consequences for the provision of information. The idea of consent was introduced in data protection law to facilitate data subjects' active choice and control, but it somehow missed that goal. Due to the increasing number of consent requests in today's world, users often do not really consider the questions asked, do not read the information provided, and do not seem to think through the consequences of providing (or refusing)

---

[735] Mark Gazaleh, 'Online trust and perceived utility for consumers of web privacy statements' *(wbsarchive.files.wordpress.com,* August 2008). See also ARA Bouguettaya and MY Eltoweissy, 'Privacy on the Web: Facts, Challenges, and Solutions' (2003) 1 IEEE Security & Privacy 40.

[736] In some exceptional cases the information duty can be fulfilled in some other ways, meaning, neither in writing nor electronically. An example is when information is provided through a provision in a law. This exception is expressly provided in articles 12 and 13 of the GDPR.

[737] Kuner (2012) 283.

[738] Ibid.

[739] However, multiple updates preceding 25 May 2018, pointing at new privacy-protecting measures, proved counter-productive. The result was an information overload contributing to confusion of data subjects rather than increased transparency. For a critical view see Esther Keymolen, 'Jouw privacy is belangrijk voor ons', *(Bij Nader Inzien,* 23 May 2008) <https://bijnaderinzien.org/2018/05/25/jouw-privacy-is-belangrijk-voor-ons/> accessed 30 May 2018.

[740] Kosta (2013) 215.

[741] See more in: Mike Hintze, 'In Defense of the Long Privacy Statement' (2015) 76 Maryland Law Review 1044.

[742] Kuner (2012) 282.

[743] See for instance the report by Alsenoy and others (2015) that was used as a basis for the investigation in Belgium. Samuel Gibbs, 'Facebook disputes Belgian tracking order over use of English in court ruling' *The Guardian* (29 January 2016) <https://www.theguardian.com/technology/2016/jan/29/facebook-belgian-tracking-english-court-ruling-cookie-browser> accessed 6 June 2018. In relation to Tinder see n 232. In relation to Google see the letter from the Article 29 Working Party from 23 September 2014 <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf> accessed 6 June 2018. The Article 29 Working Party also sent a letter to Microsoft regarding some privacy issues in their service agreement.

[744] See for example the Article 29 Working Party's letter to Google regarding their Google glass technology signed by several data protection authorities worldwide <https://www.cnil.fr/sites/default/files/typo/document/Letter-to-Google-regarding-Glass.pdf> accessed 5 June 2018.

consent; rather, they simply consent whenever confronted with a consent request.[745] If, for this reason, consent has no more meaning for data subjects' control, the same goes for the right to information that is attached to consent. Thus, it is not surprising that privacy policies as a form of communicating information have received much criticism.[746]

A few solutions have been considered to address these drawbacks and some of them have been implemented in the GDPR. These solutions do not set a new paradigm, but instead represent a sort of replacement for traditional privacy policies. The first one is the use of icons and labelling as a means to more effectively communicate privacy policies. In Article 12 of the GDPR, controllers are explicitly allowed and given an option to use icons as a replacement for written policies. The second solution is the use of standardised contract terms or templates in business-to-consumer (B2C) relationships. Standardised policies were part of some previous versions of the GDPR but do not appear in its final text. Each of the two alternatives is briefly considered below.

5.3.3.1.1. Icons and other visualisations

Icons are symbolic or graphic representations of (parts of) privacy policies that convey information at a glance. As such, they could be one possible response to the failure of privacy policies in the data economy, which are typically too long and too complex to provide meaningful information. Icons could be beneficial for two reasons in particular: first, they simplify understanding of the information, and second, they save readers time. The idea is explicated in Article 12(7) of the GDPR, which contains the option to use standardised icons. Recital 58 adds that visualisation should be used *'where appropriate'.* Icons offer an alternative approach that intends to make privacy policies more accessible to a layperson.

The GDPR does not offer much guidance concerning the icons. Article 12(7) states that the information from Articles 13 and 14 may be provided in combination with standardised icons to provide a meaningful overview of the intended processing in an easily visible, intelligible, and clearly legible manner. The article further stipulates that where the icons are presented electronically, they shall be machine-readable.

The European Commission has been entrusted with drafting the detailed guidelines on icons.[747] It is plausible that its draft will rely on the foundation set by the LIBE version of the GDPR, which introduced, in Annex 1, a first sketch of privacy icons.[748] However, it remains to be seen what approach the EC will take in the future.

---

[745] Schermer, Custers and van der Hof (2013) 1.

[746] The problem is exacerbated on mobile sites where reading long policies is impractical. Lilian Edwards and Wiebke Abel, 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors' (2014) 6 <https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf> accessed 6 June 2018.

[747] In the original version of the proposal the Commission's role to adopt delegated acts was considerably broad (*supra* n 30, see for instance articles 14(7), 15(3), 17(9) and 20(5) of the proposal). Not only was the Commission authorized to specify the use of icons, it was also assigned some other standardisation tasks. In the LIBE (Parliamentary) version, the Commission maintained those powers, but was more dependent on the European data protection board composed of national DPAs. Namely, the Parliament believed that DPAs have more specific practical knowledge and are therefore more capable of setting appropriate criteria. *Supra* n 662. In the final, adopted version, the EC's influence shrank again as the version additionally limited the number of delegated acts.

[748] *Supra* n 662.

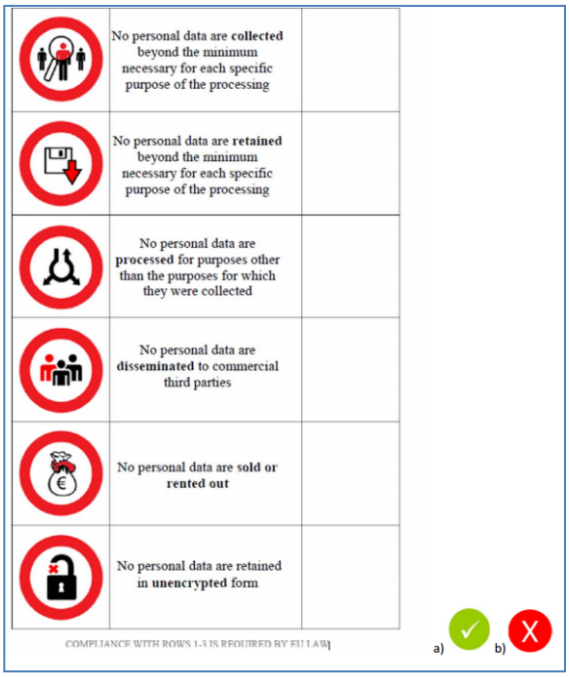

Figure 2: Privacy icons

The EC delegated acts are not the only source that companies can use to ensure that their policies are more user-friendly. Some alternative tools are also available, such as 'visuele voorwaarden' (visualised terms and conditions): a visualisation strategy created as part of a research project funded by the city of The Hague.[749] Visualisation has also been suggested as a possible way to include information on automated decision-making in a privacy policy.[750] A similar approach is to embed a privacy policy in a video.[751] Finally, information on data protection can also be provided in a more innovative manner. One example is to present a policy as a sort of nutrition label in a standardised tabular format to allow users to learn where to look to find information in a consistent location, and to facilitate comparison between policies.[752] The second example is policy compressed into a graphical representation of data flows built on AI textual analysis.[753]

Research indicates that visualisation can help some consumers better understand complicated data flows. Cranor's study found that in the condition without privacy icons, most participants made their purchases from the least expensive websites. However, in the conditions where privacy indicators were present, a significant number of participants paid extra to buy the items from the more privacy-protective web sites.[754]

---

[749] Janneke Boerman, 'Visual legal privacy statements' Presentation at the Open Minded (Leiden, Centre for Law and Digital Technologies (eLaw), 26 May 2016). For the visualization see <https://share.proto.io/FBR87S/> accessed 6 June 2018.
[750] Edwards and Veale (2017).
[751] The Guardian Privacy Policy <https://www.theguardian.com/info/video/2014/sep/08/guardian-privacy-policy> accessed on 6 June 2018.
[752] Lorrie Faith Cranor, 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2011) 10 Journal on Telecommunication & High Technology Law 273, 288.
[753] <https://pribot.org/polisis/> accessed on 6 June 2018.
[754] Lorrie Faith Cranor (2011) 292.

In solving the problems of information overload, lack of sufficient time and attention devoted to privacy-related information, and lack of digital literacy, icons and similar simplification methods could play a key role. As stated above, icons are beneficial for two reasons. First, they dramatically reduce the information overload that consumers face in the contemporary online environment. Closely related to this, they decrease information complexity. As a result, less time and attention are necessary for consumers to grasp the implications of the disclosure of their personal data.

The drawback is that icons do not provide comprehensive knowledge about data collection practices: they only provide information in a manner that is highly generalised and simplistic. By using a standardised language that signals trust, consumers may be less susceptible to the fact that they only receive partial information. However, in the data economy, it is the hidden and intangible details that carry significance rather than some general information.[755] By focusing too much on providing easy-to-understand information, individuals might be tempted to take suboptimal decisions.[756]

5.3.3.1.2. Standardised privacy policies

A regulated privacy policy in a standard form has been recommended as an effective means to ensure that consumers are sufficiently protected against industry terms that are unfair and/or significantly weighted in favour of the provider.[757] Regulating the shape of a contract is an approach that has similar consequences as icons: decreasing complexity of policies, cutting down the time needed to review the terms, and generating control for consumers (including related aims such as trust and confidence). The GDPR icons mentioned in the previous section are an example of visualised standards. Likewise, standardisation is possible for textual policies. For example, the US Glemm-Lech bill's annex provides a privacy policy template for financial institutions.[758] The LIBE version of the GDPR suggested a similar approach for privacy policies.[759] However, this provision was removed from the adopted version of the GDPR.[760]

Building on the American experience, Cranor speaks strongly in favour of standardisation.[761] She believes that the digital online environment can be a good facilitator of standardisations since

---

[755] Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140 Dædalus, the Journal ofthe American Academy of Arts & Sciences 32, 36.

[756] For example, an icon may state that no personal data is sold to third parties. However, aggregated data might still be sold and may have adverse privacy or other implications.

[757] Edwards and Abel (2014) 31.

[758] <https://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform_optout.pdf> accessed 6 June 2018.

[759] *Supra* n 662, Amendment 109. Such standardized policies/notices would include the information on whether:

- personal data are collected beyond the minimum necessary for each specific purpose of the processing;
- personal data are retained beyond the minimum necessary for each specific purpose of the processing;
- personal data are processed for purposes other than the purposes for which they were collected;
- personal data are disseminated to commercial third parties;
- personal data are sold or rented out;
- personal data are retained in encrypted form.

[760] An important addition in the LIBE version was that privacy policies should be provided in a layered form. In a layered privacy notice, basic information is provided in a short initial notice and further, more detailed information is available should an individual want it. Layered privacy notices provide an ideal way, particularly in an online context where, click through links can be adopted by providing a simple way for the data subject to access more detailed information. Supra n 662, Amendment 109, Article 13(a)(2). Also see Ustaran and International Association of Privacy Professionals (2012) 120-121.

[761] Which would, similarly as food labels, educate consumers about possible risks.

machine-readable policies allow for more standardisation and better comparison. In fact, open software already exists that supports comparisons and assessments of privacy policies.[762]

However, it cannot be excluded that visualised or standardised privacy policies could suffer from similar drawbacks as the non-standardised: either they could become too generalised and therefore miss some important details,[763] or they could become too detailed and impossible to follow.[764] More importantly, to be effective, standardised notices need to have fairly rigid requirements so that their elements are directly comparable.[765] To achieve this, a considerable amount of regulatory effort is indispensable. Ideally, standardisation is triggered by law (international treaty), by industry groups, or by standard setting bodies such as the ISO.[766] All these strategies require a lengthy negotiation process with many compromises and, as seen in the GDPR example, no guarantees of actual positive outcomes.

5.3.3.1.3. Information incorporated in standard terms and conditions

Privacy policies are by far the most common approach to inform data subjects online. However, this is not required under the GDPR. Instead of using privacy policies, some companies may choose to provide the information on personal data processing in their standardised terms and conditions (STC). The STC stand for a contract between two parties, where the terms and conditions of that contract are set by one of the parties and the other party has little or no ability to negotiate more favourable terms and is thus placed in a 'take-it-or-leave-it' position.

In principle, a privacy policy provided as part of a contract should not be considered unusual. When consent is the ground for fair and lawful processing, it is actually easy to put any data protection practice into a contract and legitimise it through acceptance of the contract.[767] However, the Article 29 Working Party advises against inserting the information in the general conditions of the contract,[768] as in digital services consent is often routinised and automatic.[769]

However, even if there is a privacy policy in place, terms and conditions might still be a source of information important to a data subject, as they might indirectly relate to the subject's privacy. For example, Twitter's APIs[770] allow developers to use Twitter's data streams.[771] A data subject can only fully understand all the risks of personal data processing by receiving the information about developers' possibilities to reuse data. In certain cases, for instance, deletion of tweets that include personal data is not absolute, as the data has already been shared with developers.[772] By combining the privacy policy and the terms, a data subject can see a more holistic picture.

---

[762] See for instance <https://tosdr.org>.
[763] Hintze (2015) 16.
[764] Omri Ben-Shahar and Carl Schneider, *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2014).
[765] Cranor (2011) 305.
[766] Edwards and Abel (2014) 4.
[767] Ibid., 6.
[768] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) 14.
[769] Edwards and Abel (2014) 6.
[770] API stands for application program interfaces.
[771] Twitter's Developer Agreement <https://developer.twitter.com/en/developer-terms/agreement> accessed 6 June 2018.
[772] Helena Ursic, 'The Right to Be Forgotten or the Duty to Be Remembered? Twitter Data Reuse and Implications for User Privacy' (2016) <https://bdes.datasociety.net/wp-content/uploads/2016/10/Ursic-politiwoops.pdf> accessed 6 June 2018.

5.3.4. Timing

5.3.4.1. When in time?

If personal data is not obtained from a data subject but from a third party, the controller has to ensure that information is received before that data is disclosed to a recipient (Article 14(3)) or at the time of first communication with the data subject if communicating is the primary reason for data processing (Article 14(2)). In other situations, the data subject has to be informed within a reasonable period, at most one month (Article 14(1)).[773]

The differences between the situations could create an interesting discrepancy. If a data controller does not intend to disclose the data (i.e., share the data with a third party), data subjects must be informed within a reasonable period, at least within one month. If the controller records the data with the intention of disclosing (sharing) it at some point, a situation which is more likely to have a significant impact on the data subject, providing the information may be delayed until the time of disclosure, however distant this might be.[774] In today's data-driven economy, where privacy risks occur mostly when data is shared and disclosed, distinguishing the situations in this manner could raise concerns.[775] To protect data subjects, the provisions should be read cumulatively.

5.3.4.2. How often in time?

In cases when data is collected directly from a data subject, the information needs to be provided at the moment of data collection (Article 13(1) of the GDPR). This information must be updated if the purpose of the data processing changes (Article 13(3)). For example, if a communication service provider starts using individuals' location data to make predictions about their shopping habits to place ads instead of using it for billing purposes only, data subjects should receive an update about that new purpose.

A distinct question is what happens if not the purpose but some other aspect of data processing changes**.** The Norwegian Consumer Council's (NCC) report supports a broader interpretation, under which all updates should be communicated*: 'Especially in the case of material changes, including functionality and user rights, the services should provide advance notice, so that anyone who does not agree to the new terms has an opportunity to export their data, leave the service, and potentially find*

---

[773] *'It must, however, be observed that that provision, which concerns data which have not been obtained from the data subject, provides for information to be provided to the data subject not at the time when the data are obtained but at a later stage. By contrast, Article 10 of Directive 95/46, which refers to the collection of data from the data subject, provides for the data subject to be informed at the time the data are collected […]. The immediate nature of the provision of information to the data subject thus comes not from Article 11 of Directive 95/46, mentioned by the referring court, but from Article 10.'* Case C-473/12, *IPI v. Geofrey Engelbert* ECLI:EU:C:2013:715 (7 November 2013), para. 23.

[774] Douwe Korff, 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws' (2002) <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE> accessed 6 June 2018.

[775] On a similar note, one could raise doubts in the system in which the timing of the communication with a data subject is based merely on the fact whether data is obtained from a data subject or not. Apart from some practical difficulties that controllers could face, there is no reason to demand that in one case information is provided right away while in the other (and potentially more invading) situation, the provision of information can be delayed for a few weeks. For example, communicating information about future recipients of data is necessary before data is obtained from a data subject. In cases when data is received from a third source, however, article 14(3)(c) suggests that this can be done up to the moment when data is disclosed to a new recipient.

another provider before the new terms are put into effect.'[776] To summarise, in the NCC's view material changes should always be communicated, but a note to consumers should not be ruled out in the case of minor changes.

The Article 29 Working Party believes that it is a precondition for the exercise of data subject rights that individuals be continuously kept informed, not only when they subscribe to a service but also when they use it. For example, if a service requires ongoing processing of location data, the Working Party takes the view that the service provider should regularly remind the individual concerned that her terminal equipment has been, will be, or can be located. This allows that person to exercise the right to withdraw, should she wish to do so.[777] In line with the Working Party's view, any other relevant change that might urge data subjects to withdraw or block certain processing of personal data should also be regularly provided as an information update.[778]

5.3.5. Restrictions

Because the right to information is a manifestation of the fundamental right to data protection and some other fundamental principles,[779] every exception has to be used with the utmost prudence and care. According to the settled case law, *'the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.'*[780]

The GDPR's provisions on exceptions try to establish the right balance between legitimate interests of data controllers and protection of data subjects. The most obvious exception to information duty applies when a data subject already has all the information to which he is entitled (Article 13(4)). In such cases, providing the information for the second time is neither necessary nor economical.

In cases when data is *not* obtained directly from a data subject, the GDPR offers some further exceptions in addition to the one explained in the paragraph above. For example, the information duty is limited if it would require disproportionate effort, especially when data is used for archiving in the public interest, for scientific or historical research purposes, or for statistical reasons.[781] Consider researchers employing a medical data set for new scientific research unrelated to the data's original use. Given the size of the database and, more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually to provide them with the information on the new purpose of use of the database.[782] Thus, an exception should apply.

---

[776] Forbrukerradet, 'Consumer Protection in Fitness Wearables' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf> accessed 5 June 2018.
[777] Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent' 33.
[778] Ibid.
[779] Such as transparency and fairness. See section 5.2. of this chapter for more detail.
[780] See for example Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831, paragraph 56, and Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paragraphs 77 and 86.
[781] Article 14(5)(b) and (c). The scope of 'scientific research' is not clear. Whether pharmaceutical research also falls under this exception is open to discussion. According to the interview with a pharmaceutical company representative, if the RWE initiative is not scientific research *per se*, it could be at least something *that adds to scientific research*. In this way, also pharmaceutical research could fall under the umbrella of Article 14. Liliya Pullmann and others (2017) 32-33.
[782] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) 31.

Interpreting open terms such us 'disproportionate' can be challenging in certain cases. Should disproportionate be understood objectively or subjectively? Disproportionate effort has a different connotation for a large commercial company that plans to utilise personal data to increase sales than for an understaffed academic centre. Through the eyes of the Google Spain court, balancing fundamental rights should disregard economic difficulties of a data controller.[783] It is likely that the bar to avoid information duties should be set higher for commercial companies.

The exceptions listed above are specific to the right to information. Article 23 of the GDPR contains an additional set of exceptions such as national security and public interest that are applicable to all data subject rights.[784] Therefore, they should also be read jointly with Articles 13 and 14.

5.4. The right to information in the electronic communication sector

5.4.1. Privacy of electronic communication

Therefore, the information duty from the GDPR applies equally to all controllers of personal data regardless of sector. However, protection of personal data in the electronic communication sector is additionaly safeguarded by ePrivacy rules. Inasmuch as the ePrivacy rules provide specific rules in relation to electronic communications, this additional or special provision should also be taken into account on top of the GDPR rules. This situation is a specific application of the doctrine stating that a 'law governing a specific subject matter (*lex specialis*) overrides a law which only governs a general matter (*lex generalis*).'[785]

The current 2002 ePrivacy directive will soon be replaced by a new regulation intended to bring (sometimes clashing) national legislations closer to each other.[786] At the time of writing, the text of the regulation was still in the legislative procedure, but based on the EC proposal some of the positive and the negative points could already be assessed.[787] The text below provides an overview of the ePrivacy

---

[783] '*In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing*.' C-131/12, *Google Spain,* ECLI:EU:C:2014:317.

[784] Under Article 23 of the GDPR restricting data subject rights may be allowed under the principle of proportionality. In other words, the restricting measure has to be laid down by law, respect the essence of the fundamental rights and freedoms, and fall under the limits of proportionality test, i.e. be necessary and proportionate in a democratic society to safeguard the following objectives:

- national security;
- defence;
- public security;
- criminal prevention and enforcement
- other important objectives of general public interest of the Union or of a Member State e.g. financial or economic interests
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

[785] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' 10.

[786] In the system of EU law, regulation is a type of law that intends to unify rather than harmonize national legislations. In other words, when a regulation is adopted its text is in principle directly implemented in member states. Directives, on the other hand, are only binding as far as their goals are concerns, but still allow for divergences.

[787] *Supra* n 468.

law in relation to information rights, drawing mainly on the ePrivacy directive. When specific provisions are discussed, it is indicated whether the directive or the regulation is referred to.

The ePrivacy rules concern four types of data processing: (1) processing of traffic data, (2) processing of location data, (3) using electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user, and (4) other uses, such as unsolicited messaging and telephone calls as part of direct marketing, and inclusion in public directories.

In the context of the data-driven economy, the last type (4) is less relevant. The other three, however, represent an integral part of modern personal data processing, especially in the online environment. To illustrate the application of the right to information in the electronic communication sector, the following sections briefly introduce the information duty in relation to the third type (3) of e-communication data processing. Within this group, it is possible to distinguish two types of processing: (a) storing information in the terminal equipment of a subscriber, and (b) gaining access to the information stored therein.[788]

5.4.2. Informing about placing the cookies and location tracking

Within the scope of (3) above (storing information in the terminal equipment of a subscriber), ePrivacy provisions restrict the use of cookies and/or similar technologies (e.g. web beacons, Flash cookies, etc.)[789] stored on users' computers to track their online behaviour.[790] This type of personal data processing is a building block of the e-commerce online advertising business. By storing a cookie on a user's computer, advertisers obtain a precise understanding of this person's actions on the Internet. As a consequence, they are able to direct their ads to the most interested (or most vulnerable) consumers and therefore increase their sales. Considering the exponential growth of the e-commerce sector, it is likely that online behavioural advertising and the use of cookies and similar technologies will expand in the future.[791,792]

Under current (and upcoming) ePrivacy rules, deploying cookies is only allowed if data subjects have consented to it and if they have *'been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing'*[793] Thus, providing information and obtaining consent form an indivisible whole. Informing the data subject should take

---

[788] See Article 5(3) of ePrivacy directive.

[789] A web beacon is a small, invisible object such as a tiny clear image that is the size of a pixel embedded into a web page. When a web page with this image loads, it will make a call to a server for the image. This is very useful to companies that want to learn if readers are opening the emails they send. A flash cookie is a piece of information that Adobe Flash might store on your computer to save data such as video volume preferences or, perhaps, your scores in an online game. Flash cookies are more persistent and cannot be deleted in the same way as other cookies. Joanna Geary, 'Tracking the trackers: What are cookies? An introduction to web tracking' *The Guardian* (23 August 2012) <https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro> accessed 23 September 2018.

[790] See Article 5(3) of ePrivacy directive and Article 8 (1) of the proposal for the ePrivacy regulation.

[791] Robert Gebeloff and Karl Russell, 'How the Growth of E-Commerce Is Shifting Retail Jobs' *The New York Times* (6 July 2017) <https://www.nytimes.com/interactive/2017/07/06/business/ecommerce-retail-jobs.html> accessed 6 June 2018.

[792] Recently, researchers have found that 100 most popular sites collect more than 6,000 cookies, of which 83% are third-party cookies, with some individual websites collecting more than 350 cookies. Ibrahim Altaweel, Nathaniel Good and Chris Jay Hoofnagle, 'Web Privacy Census' [2015] Technology Science.

[793] Article 5(3) of the e-Privacy directive. The proposal for the ePrivacy regulation refers to the GDPR's provision on the right to information (Article 8(1)(b) of the proposal).

place before the server of a controller sends the cookie to the Internet user's hard disk.[794] In practice, this is normally done by using a cookie banner. Cookie header banners are displayed on websites using cookies and require consent if a user wants to proceed to the website. Such cookie banners easily turn into a 'take-it-or-leave-it' option. As a result, the majority of users consent whenever they are confronted with a cookie wall.[795] Due to lack of *informed* consent, it has been suggested that tracking walls should be banned, at least in certain circumstances.[796] Instead, browser and comparable software settings could play a role in addressing this problem. For instance, it has been argued that browsers could be set to privacy-friendly settings that limit online tracking.[797]

Besides the medium used to convey the information, the content of the message is equally important. In relation to automated online data collection (e.g. cookies), the Article 29 Working Party suggested that data subjects should be provided not only with the standard set of information listed in Article 13 of the GDPR, but also with some extra items.[798] In a document from 2013, the Working Party stated that the necessary information regarding cookies includes the purpose(s) of the cookies and, if relevant, an indication of possible cookies from third parties or third-party access to data collected by the cookies on the website.[799] For example, if a cookie is used to remember in what language version an Internet user wants to access a website, then the information should explain that and notify the user that the next time he visits he will not have to repeat his choice, since it will be remembered by the cookie.[800] In addition, if the information is gathered or processed by third parties, then this fact should be pointed out specifically to Internet users.[801] Marketers should also convey additional information (or link to it) regarding who that third party is and how it may use the information.[802] Information such as retention period (i.e. the cookie expiry date), details of third-party cookies, and other technical information should also be included to fully inform users.[803] Finally, in the Working Party's view, users must be informed about how they can signify their wishes regarding cookies, i.e., how they can accept all, some, or no cookies, and how they can change this preference in the future.[804]

Tailoring the information to the nature of a specific technology is a good strategy that should be adopted for other technologies as well (e.g., Wi-Fi tracking, face and voice recognition by IoT devices). However, informing users about cookies leads to exactly the same problems as any other type of

---

[794] Article 29 Data Protection Working Party, 'Recommendation 2/2001 on Certain Minimum Requirements for Collecting Personal Data on-Line in the European Union' 6.

[795] Frederik Johannes Zuiderveen Borgesius and others, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' (2017) 87 <https://www.ivir.nl/publicaties/download/IPOL_STU2017583152_EN.pdf> accessed 17 November 2017.

[796] Ibid., 89. Negotiations on whether cookie walls should be prohibited or not are still ongoing.

[797] Ibid., 8.

[798] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' 3.

[799] UK Information Commissioner Office, 'Guidance on the Rules on Use of Cookies and Similar Technologies' 21 <https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf> accessed 17 November 2017.

[800] Ibid.

[801] Ibid., 22-23.

[802] Ibid.

[803] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' 3.

[804] Ibid. See also International Chamber of Commerce UK, 'ICC UK Cookie Guide' <https://www.cookielaw.org/media/1096/icc_uk_cookiesguide_revnov.pdf> accessed 7 June 2018; Informacijski pooblaščenec Republike Slovenije, 'Kdaj Lahko Uporabimo Piškotke? Smernice Informacijskega Pooblaščenca' <https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_uporabi_piskotkov.pdf> accessed 7 June 2018.

communication to data subjects. When the information is short and summarised, some important details may be missed, while when it is long and detailed, it is perceived as a burden and often disregarded. Although there is no simple solution to data subjects' disinterest, providing a complete set of facts is not useless. The information may be useful to regulators, journalists, and the general public, and thus work as an important indicator of a controller's accountability.

5.4.3. Informing users about Wi-Fi tracking

Within the scope of (3)(b) above (gaining access to the information stored in a subscriber's terminal equipment) ePrivacy law regulates location tracking on the basis of Wi-Fi or Bluetooth signals emitted by people's smart phones. Under the ePrivacy directive, this is only allowed if data subjects have consented to it and have been provided with clear and comprehensive information. Under the proposed ePrivacy regulation,[805] such tracking is allowed under somewhat relaxed conditions (Article 8(2)). Article 8(2) states that in order to inform those who are being tracked, it is sufficient to display a clear and prominent notice, e.g. hang a poster with information about the tracking. This means that collection of valuable data is in principle possible without the hassle of obtaining individuals' consent. Some retail stores have already successfully embraced this as the new technique to monitor shoppers.[806] For this reason, Article 8(2) has been fiercely criticised for not sufficiently allowing data subjects' control and intervening with some broader privacy objectives. Clearly, providing a poster with some general information does not resolve privacy risks in relation to tracking. *'Under that proposed rule, people might never feel free from surveillance when they walk or drive around. People would always have to look around whether they see a sign or poster that informs them of location tracking*.'[807] The Article 29 Working Party assessed the proposal and issued a negative opinion, urging the legislator to only allow Wi-Fi tracking on the basis of informed consent.

5.4.4. Information on cybersecurity

The draft ePrivacy regulation introduces a new obligation for electronic communications service providers to provide information about the security of their technology, e.g. about using encryption. Article 17 stipulates: '*In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken*

---

[805] *Supra* n 468.

[806] *'Everything from where they go, what they look at, how long they engage with a product and whether all this ultimately results in a sale, can all be anonymously monitored and used to make each experience more personal.'* Sarah Knapton, 'High street shops secretly track customers using smartphones' *The Guardian* (27 December 2016) <http://www.telegraph.co.uk/science/2016/12/27/high-street-shops-secretly-track-customers-using-smartphones/> accessed 7 June 2018.

[807] Zuiderveen Borgesius and others (2017) 8. Another degradation of data protection related to the information duty can be spotted in Article 10 of the proposed ePrivacy regulation from December 2016. The draft proposal that was leaked in December required that any setting of terminal equipment (e.g. personal computer, mobile phone) must be configured in a way that prevents third parties from storing information in this equipment, or to use information that has been stored there. In essence, the requirement demanded that third party cookies, which are the backbone of the targeted advertising industry, should be blocked by default. The later proposal abolished this requirement. Rather than requiring that the software is set to "do not track", privacy-friendly mode, the official proposal only requires that it *offers an option* to do so and provides information about this option. Again, the provision was criticized as it is obvious that merely informing someone offers far less privacy protection than creating privacy-enabling software architecture. Helena Ursic, '"The bad" and "the good" of ePrivacy proposal' (*Leiden Law Blog,* 19 January 2017) <http://leidenlawblog.nl/articles/the-bad-and-the-good-of-the-eprivacy-regulation-proposal> accessed 3 June 2018.

by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.' According to Recital 37, this information should be provided free of charge.

Given the rising number of cyber risks, stronger reference to security can have positive consequences for data subjects' awareness and control. However, it has been argued that ePrivacy regulation is not the best setting to regulate cyber risk.[808] Notably, cyber security is already addressed in some other legal acts, including the GDPR.[809] Lack of reference to these acts in the ePrivacy regulation might be puzzling. In addition, security of devices is a technical and complicated topic that cannot be thoroughly dealt with in the ePrivacy regulation.[810]

5.5. The right to information as a control affording entitlement

This section summarizes some key barriers and enablers to providing meaningful information that have to some extent already been crystallised in the previous sections. The aim is to assess the degree to which the right succeeds or fails at helping data subjects exercise control over their personal information.

5.5.1. Limits to data subjects' control

In section 4.5, it was suggested that three groups of factors – psychological, technological and economic – seem to undermine the effectiveness of data subject rights and escalate data subjects' inability to control information flows. As shown in section 5.1.-5.4., these same factors also have implications for the right to information. The barriers to providing effective information stem from individual psychological patterns, the specifics of data-driven technologies, and the modern economic environment.

Psychological factors. The ubiquity of personal data processing in combination with the information duty has resulted in the phenomenon of informational overload. Today, the majority of modern devices, media, and services use personal data. Since almost every use of personal data triggers the right to information, consumers are confronted with major amounts of information about their personal data processing daily. The continuous (though partial) attention to an increasing amount of information decreases data subjects' ability and motivation to scrutinise the key details that are necessary to make informed privacy decisions. Paradoxically, the more information they receive, the less information they are able to filter, process, and weigh to make decisions that are in line with their preferences.[811] Further, limitations in general cognitive abilities and low 'literacy' prevent data subjects from understanding the complex policies' language.[812] The phenomenon of 'bounded rationality' also adds to the problem: this concept confirms that judgements and decisions are often not reached on the basis of a rational *optimisation process*, but are instead the result of heuristic and biased

[808] Zuiderveen Borgesius and others (2017) 106.
[809] Notably the NIS directive, *supra* n 475.
[810] Ibid.
[811] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2016] TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016.
[812] Eszter Hargittai, 'Whose Space? Differences Among Users and Non-Users of Social Network Sites' (2008) 13 Journal of Computer-Mediated Communication Whose 276.

information processing.[813] For example, the mere existence of a privacy policy signals trustworthiness, which in turn decreases privacy concerns and increases disclosure behaviour.[814]

Technological fators. The intangible and invisible nature of personal data opens up possibilities to duplicate and share in an opaque and less controlled way than physical goods. This specific technical nature of data challenges the simple disclosure mechanisms suggested in the GDPR. It is the hidden and oftentimes highly technical details that carry significance.[815] The Article 29 Working Party describes this problem in a mobile app environment. While apps can have extremely broad access to sensors and many other data structures on a device, in many cases this access is not intuitively obvious.[816] Moreover, after data is collected, it can easily flow to third-party data controllers or processors, where it is combined and/or reused.[817] The route that personal data takes is difficult to follow. Often, even the data collector itself is ignorant of the parties that eventually receive it.[818] This of course challenges transparency of data processing. Simplifying privacy policies by using plain and concise language as suggested in the GDPR will probably make them easier and quicker to read, thus mitigating the psychological problem of information overload and bounded rationality, as described in the previous section.[819] However, when it comes to the complexity of data flows, simplification is not of much help. Control will almost never stem from the information provision, but will only come from external overseeing of data processing practice such as academic research and enforcement checks.

Economic factors. Finally, the right to information is challenged by the diffusion of responsibility. In the modern data economy, the tendency to reuse data creates a network of multiple actors involved in the processing of the same data. This technical diffusion of responsibility is also economically incentivised by the underlying business models such as behavioural advertising.[820] Consequently, the duty to inform becomes dispersed. For example, data can be purchased from a third party, such as a data broker, and can then be curated, repackaged, and sold to another party. In such cases, a data subject often has no interaction with the actual controller.[821] Although individuals maintain the right to information, the timing and the scope of the received information is influenced by the fact that data flows through a network of (joint) controllers and processors. When information is received from a third party, the set of information is to some extent limited and is not presented directly to a data subject.[822] Clearly, such

---

[813] Gigerenzer and Selten (2002).

[814] A study by Hoofnagle and Urban found that 62% of respondents to a survey believed that merely the existence of a privacy policy on a website implied that this website was not allowed to share their personal information without permission. Chris Jay Hoofnagle and Jennifer M Urban, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest L. Rev. 261.

[815] Nissenbaum (2011) 36.

[816] Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' 22. Also see Section 5.4.3. of this chapter.

[817] Ellen Nakashima, 'Prescription Data Used to Assess Consumers' *The Washington Post* (4 August 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080302077.html> accessed 5 June 2018.

[818] Ursic (2016). Also see hearing of Mark Zuckerberg in the US Congress on April 10, 2018 (n 642) for the report on apologies made by Facebook CEO Zuckerberg for not discovering inappropriate data flows triggered by Cambridge Analytica's app.

[819] The problem of bounded rationality will be difficult to solve with the measures that supposedly increase the scope or quality of communication. Rather, a modification of the software architecture should be deployed as the solution – for instance, a default option that is privacy friendly and an opt in requirement. However, under the pressure of the industry lobby, regulators are typically hesitant in adopting such radical measures.

[820] Section 2.3.3.

[821] See section 2.3.1. in relation to the data brokers' business model.

[822] See section 5.3.1.1.

conduct decreases control over data processing. Furthermore, exceptions to the right enable controllers to escape the information duty when it would involve disproportionate efforts.[823] As it appears, the disproportionality is most likely to be asserted in relation to providing the information that proves highly relevant in the context of data reuse. For instance, providing thorough information on recipients (second, fourth, fifth, etc.) and data sources would typically require disproportionate efforts.

5.5.2. Enablers to data subjects' control

Paraphrasing Westin, effective control encompasses mechanisms that have two goals: helping individuals understand (1) *where* their personal information may flow and (2) *under what conditions* it may flow.[824] The right to information pursues both goals. To understand the location of data, controllers must communicate the details on recipients of data, international transfers of data, and data storage. To understand under what conditions the data flows, the GDPR informs users on the legal basis and the purpose of data processing. In the past, understanding of the flows may have been sufficient to achieve effective control. However, today's economic reality is more complex and disguised, and having control is more difficult. To address this issue, the GDPR has extended some existing provisions and introduced some new provisions intended to strengthen data subjects' control in the data-driven economy. These new mechanisms are, among others, the right to explanation and icons.

The so-called right to explanation was seemingly introduced in the GDPR to address the problem of incomprehensibility of data-driven decisions. Technical complexity of algorithmic decisions often makes it impossible to explain how exactly data was used. This is why the right to explanation encompasses not only a requirement of meaningful information but also information about the significance and consequences for an individual. This change is promising, although it does not come without problems, such as difficult implementation and limited scope.

The right to explanation is only the starting point of an EU journey towards a more comprehensive regulatory framework for AI. Within the GDPR, the new right to explanation is enhanced by some other relatively new overarching provisions on accountability, fairness, and transparency, and by more tangible requirements such as that on the privacy impact assessment. In addition, AI decisions will probably be tackled as a separate initiative on the EU level. It has been suggested that a general framework on algorithmic accountability and transparency could importantly strengthen consumers' rights. Liisa Jaakonsaari, an EU MP, recently proposed '*a general framework on algorithmic accountability and transparency*' that could be the next step in achieving these goals without raising unrealistic expectations regarding the right to information in the GDPR.[825] Furthermore, the EC just

[823] Article 14(5)(b) of the GDPR.
[824] Westin (2015) 5.
[825] Lisa Jaakonsaari, 'Who sets the agenda on algorithmic accountability?' *EURACTIV* (26 October 2016) <https://www.euractiv.com/section/digital/opinion/who-sets-the-agenda-on-algorithmic-accountability/> accessed 7 June 2018. Jaakonsaari also warns of the fact that the right to explanation only applies to a relatively narrow segment of algorithmic decision-making, as the definition of "solely automated" can be circumvented.

recently created the European Group on Ethics in Science and New Technologies, which has been entrusted with the task of examining the needs for the regulation of AI.[826]

Icons can be seen as another enabler in the sense that they bring an additional option for consumers who prefer visualisations, and that they replace complex privacy policies by a series of simple images. The introduction of icons and some related mechanisms[827] in the GDPR indicates a stronger link between data protection and consumer protection. In fact, the convergence between data protection and consumer law that has been increasingly discussed is something that also works to data subjects' benefit. After all, the failure of controllers to fulfil their information duty can have adverse legal consequences, a combination of those stemming from contract law and consumer protection law.[828] In recent investigations of information duties (typically in relation to privacy policies), the authorities have required changes based on both data protection and consumer protection law. For example, the Norwegian Consumer Ombudsman requested that the users of activity trackers such as Fitbit and Jawbone be notified of changes in privacy policies and other terms, to prevent users from suddenly finding themselves having implicitly 'agreed' to something of which they had no knowledge.[829] A policy that does not respect those requirements is deemed null or void, and as a consequence consumers have a complaint or class action.[830] The bond between data protection and consumer protection policy is meant to intensify in the future. For instance, the EU Commission's proposal of the directive on certain aspects concerning contracts for the supply of digital content is the first indicator of this new regulatory vision.[831]

5.6. Conclusions

This chapter sought to answer the fourth research sub-question: *What entitlements do data subjects enjoy under the EU data protection law, what implications does the data-driven economy have for these entitlements and, specifically, how do they afford control to data subjects?* While this research question refers to data subject rights as a whole, in this chapter the scope was narrowed down to the right to information.

In the first part of the chapter, the right to information was assessed in the context of the data-driven economy. It was shown that, in particular, the information about the legal basis for data processing, third parties involved in data processing, the source of personal data, and the information about purposes of data processing are what give data subjects the most relevant information about data processing. The GDPR extends the scope of the information catalogue available to data subjects and pays more attention to user-friendly design of the form in which the information is presented. Specifically, the right to explanation and icons seem to offer a new, promising option to exercise more control over modern data flows. In spite of these novel steps in the GDPR, entitlements that the law affords are undermined due to three groups of factors: psychological, technological, and economic. In the data-driven economy, these factors seem to gain influence and have a negative impact on data

[826] <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence> accessed 6 June 2018.
[827] Provisions on the quality of information in Article 12.
[828] Kuner (2012) 286.
[829] Forbrukerradet (n 755) 9. Cases in which both types of law overlap have already been considered by the CJEU; see for example Case C-191/15, *Verein für Konsumenteninformation v. Amazon EU* [2016] ECLI:EU:C:2016:612.
[830] Kuner (2012) 286.
[831] See more in Chapter 3.

subjects' ability to control information flows. The GDPR changes are not radical enough to revolutionise the impact of the right to information. However, this does not mean that the right is a paper tiger. After all, the right to information is not addressed to data subjects only, but establishes transparency for a whole economic environment including competitors, civil society, and regulators. Post-GDPR, national DPAs have become more active in terms of spotting inappropriate information practices. Finally, the right to information is not an isolated right but is part of a comprehensive data protection and a broader EU law regime. This regime may not excel in facilitating meaningful control for an individual, but it does certainly promise one of the most granular and comprehensive data protection mechanisms to date.