Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

4 Data protection law, principles

The main legal instrument in the EU to protect privacy in the area of behavioural targeting is the e-Privacy Directive's consent requirement for tracking technologies, together with the Data Protection Directive. In January 2012 the European Commission presented a proposal for a Data Protection Regulation, which should replace the Data Protection Directive.[605] The proposal is based on the same principles as the Directive.[606] Data protection law is a legal tool, which aims to ensure that data processing happens fairly and transparently. Data protection law aims to ensure fairness, by imposing requirements on data controllers when they process personal data. Data protection law aims to protect privacy interests, but also other interests, such as the prevention of unfair discrimination.[607] This chapter provides an introduction to data protection law for the purposes of this study.

When discussing data protection law, this study draws in particular on opinions published by the Article 29 Working Party, an independent advisory body installed by article 29 of the Data Protection Directive. The Working Party consists of representatives of the Data Protection Authorities of the member states, the European Data Protection Supervisor, and a representative of the European Commission.[608] The Working Party has several duties, including advising the European Commission on

---

[605] European Commission proposal for a Data Protection Regulation (2012).
[606] See European Commission proposal for a Data Protection Regulation (2012), p. 4.
[607] Brouwer 2008, p. 194-204. Blok 2002, p. 131-132. The Impact Assessment for the proposal for a Data Protection Regulation contains a list of fundamental rights that are affected by data protection law (Impact Assessment for the proposal for a Data Protection Regulation, p. 39-40).
[608] Article 29(2) of the Data Protection Directive. The European Data Protection Supervisor (EDPS) is the supervisory authority responsible for monitoring the processing of personal data by the EU institutions and bodies (see article 41 of Regulation (EC) 45/2001 on personal data processing by the Community institutions and bodies).

EU measures affecting the rights and freedoms with regard to personal data processing.

The Working Party can also publish opinions on all matters relating to the processing of personal data.[609] Since 1997, the Working Party has published more than 200 opinions, covering topics such as the concept of personal data, consent, cookies, and behavioural targeting. The Working Party's opinions aren't legally binding, but they are influential. Although the Working Party can adopt opinions after a vote,[610] it usually makes decisions by consensus.[611] In several cases, Advocates General of the European Court of Justice have referred to the Working Party's opinions when interpretatiing data protection law.[612] Lawyers keep an eye on the Working Party's opinions when interpretatiing data protection law.[613] The European Commission proposal for a Data Protection Regulation foresees the replacement of the Working Party by a European Data Protection Board.[614] But the Working Party's opinions will remain relevant, as the Regulation uses the same terminology as the Directive.

The Working Party has been criticised, for instance, for being too extreme in its opinions.[615] And, perhaps because consensus requires compromises, the opinions aren't always crystal clear. Nevertheless, the opinions give an idea of the views of European national Data Protection Authorities.[616]

Data protection law doesn't grant property rights to data subjects. But for ease of reading this study sometimes speaks of "their data" instead of "data concerning them." The study often refers to parties that process personal data as firms or

---

[609] Article 29 and 30 of the Data Protection Directive.
[610] Article 29(3) of the Data Protection Directive.
[611] Gutwirth & Poullet 2008.
[612] See for instance Opinion AG (14 April 2011) for CJEU, C-70/10, Scarlet v. Sabam, 24 November 2011, par. 74-78; Opinion AG (25 June 2013) for CJEU, C-131/12, Google v. Spain (in this case the AG disagrees with the Working Party on some points).
[613] See Bamberger & Mulligan 2013.
[614] Article 64 of the European Commission proposal for a Data Protection Regulation (2012).
[615] See Interactive Advertising Bureau Europe 2010; Zwenne 2013, p. 36.
[616] Sometimes national Data Protection Authorities appear to follow a different course than the Working Party. See for instance chapter 6, section 4, on the English interpretation of consent.

companies.[617] Data subjects are also referred to as people, persons or individuals. Personal data are also referred to as data.

The chapter is structured as follows. Section 4.1 sketches data protection law's history. Section 4.2 provides an overview of the data protection principles. Section 4.3 and 4.4 discuss data protection law's aim for transparency and for fairness. Section 4.5 considers the tension in data protection law between protecting and empowering the data subject. Section 4.6 concludes.

4.1 History

Data protection law's focus on making data processing transparent can be partly explained by its historical background. As noted in the previous chapter, the perspective on privacy as control over personal information became popular in the late 1960s.[618] Many people were concerned about the effects of large-scale data processing by the state and other large organisations. The use of computers for data processing added to the worries. Computers could be used to make decisions about people without human input. In this context, data protection law was developed in the early 1970s. While data protection law has evolved considerably, its underlying principles have remained largely in place.[619]

In Europe, three international organisations have been particularly important for data protection law: the Council of Europe, the Organisation for Economic Co-operation and Development, and the European Union.[620] The Council of Europe took some of the earliest steps in the field of data protection law.[621] In 1968, the Parliamentary

---

[617] This is a simplification. The Data Protection Directive distinguishes "data controllers" from "data processors", but an analysis of that distinction falls outside this study's scope. See section 2 of this chapter.
[618] See chapter 3, section 1.
[619] See generally about the early history of data protection law Hondius 1975; Sieghart 1976; De Graaf 1977; Flaherty 1989; Nugter 1990; Mayer-Schönberger 1997; Rule & Greenleaf 2010; Kosta 2013a, p. 12-82; González Fuster 2014. See for a political science angle Bennett 1992; Newman 2008.
[620] Data Protection Convention 1981, Explanatory Report, par. 14-16. See also Bennet 1992, p. 130-136; González Fuster 2014, chapter 4-8.
[621] See on the Council of Europe chapter 3, section 2.

Assembly of the Council of Europe asked the Committee of Ministers to examine whether the European Convention on Human Rights offered adequate privacy in relation to "modern science and technology."[622] The study concluded that the Convention's right to private life didn't offer sufficient protection. Therefore the Committee of Ministers adopted two resolutions in 1972 and 1973, with principles for the protection of privacy in the area of digital data processing, for the private and the public sector. In its Resolutions, which aren't legally binding, the Committee of Ministers calls for member states "to give effect to the principles," and suggests that legislation may be needed.[623]

Around the same time, in several countries similar principles were developed that should apply to data processing. The principles can be found in the world's first Data Protection Act in the German state of Hesse (1970),[624] and the first national Data Protection Act in Sweden (1973).[625] In the UK and the US, comparable principles were proposed around that time, but no comprehensive data protection laws were adopted at the time.[626] (The US did, however, adopt rules for data processing in the public sector in 1974.[627]) Legislation followed in Germany (1977), France, Austria, Norway and Denmark (1978), and later in other European countries.[628]

It's impossible to establish in which country the data protection principles were developed first, says Bennett.[629] A 1974 report of the Organisation for Economic Cooperation and Development found "a striking similarity to the independent yet

---

[622] Data Protection Convention 1981, Explanatory Report, par. 4.
[623] Council of Europe, Committee of Ministers, Resolution (73)22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 September 1973; Committee of Ministers, Resolution (74)29 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the public sector, 20 September 1974.
[624] Hessisches Datenschutzgesetz [Hesse Data Protection Act], Gesetz und Verordungsblatt I (1970), 625 [repealed].
[625] Datalagen (Data Act), SFS (Svensk Författningssamling; Swedish Code of Statutes) 1973:289 [repealed].
[626] UK: Younger Committee 1972; US: United States Department of Health, Education, and Welfare 1973.
[627] The US did adopt a data protection act for the public sector (Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974), codified at 5 U.S.C. 552a).
[628] Mayer-Schőnberger,1997, p. 237 (footnote 3).
[629] Bennet 1992, p 99. See also Hondius 1975; Mayer-Schönberger 1997, p. 221.

correlative actions in data protection and privacy" in different countries.[630] The basic principles of data protection law are sometimes called the Fair Information Principles (FIPs), or the Fair Information Processing Principles (FIPPs).[631] Although the application of the data protection principles varies considerably, they express an almost worldwide consensus on minimum standards for fair data processing.[632]

According to Bennett, it isn't surprising that countries developed similar principles. Computers were developing fast, were quickly being adopted, and had a "mystical or closed quality."[633] While the general public, policymakers, and academics felt uneasy about the new phenomenon of personal data processing, the threats for fundamental rights weren't exactly clear.[634] Therefore, legislation was drafted that aimed to make data processing transparent, and to make computers and databases less mysterious. "Basing legislative action on the assumption that 'the lid must be taken off' leads data protection policy to some inevitable conclusions."[635] Data protection law aims to open the black box of data processing. Making data processing transparent should help to signal problems, which could otherwise remain invisible.

Several European data protection laws from the 1970s contained restrictions on exporting personal data. This worried some countries, the US in particular. Some feared that states would use data protection acts as a disguised trade barrier.[636] Therefore, European countries and the US negotiated about more international cooperation in the Organisation for Economic Cooperation and Development (OECD). In 1980, this led to the adoption of the OECD Guidelines for the Protection

---

[630] Organisation for Economic Co-operation and Development, 'Developments in Data Protection and Privacy by OECD Countries', Unpublished survey from the OECD's Computer Utilization Group (Paris: OECD, Directorate for Scientific Affairs, 1975), p. 2, quoted in Bennett 1992, p. 95.
[631] Especially in US literature FIPs and FIPPs are common phrases. See for an overview of the history of the Fair Information Principles Gellman 2013, which is a document that is regularly updated.
[632] The European data protection regime goes much further than the FIPs as expressed in the OECD Guidelines (see for criticism on the OECD Guidelines Clarke 2000; Clarke 2002).
[633] Bennett 1992, p. 118-119. See also p. 21.
[634] See Van Dijk 1970, p. 34; Hondius 1975, p. 4, p. 7-8, p. 80-81; Flaherty 1989, p. 373; Bennett 1992, p. 12, p. 29.
[635] Bennett 1992, p. 121. See also González Fuster 2014, p. 126.
[636] Platten 1996, p. 15; González Fuster 2014, p. 77. Similar arguments are used in the discussion about the European Commission proposal for a Data Protection Regulation (2012).

of Privacy and Transborder Flows of Personal Data. The Guidelines, which aren't legally binding, are built on similar principles as current data protection law. The OECD Guidelines were updated in 2013.[637]

In 1981, the Council of Europe adopted the first legally binding international instrument on data protection, the Data Protection Convention.[638] It entered into force in 1985, and contains similar principles to the OECD guidelines. The Data Protection Convention requires signatories to enact data protection provisions in their national law.[639] The Data Protection Convention has been supplemented with a number of recommendations, which aren't legally binding, regarding data processing in specific sectors.[640] For instance, there's a recommendation on personal data processing for direct marketing, on profiling, and on the protection of privacy and personal data on the internet.[641] The European Court of Human Rights sometimes cites such recommendations, although they're not legally binding.[642]

European Union

The European Commission had called on the European Community member states to ratify the Council of Europe's Data Protection Convention in 1981, but in 1990 only seven member states had done so.[643] Furthermore, the Data Protection Convention left possibilities for countries to raise barriers for personal data flows at the borders.[644]

---

[637] Organisation for Economic Co-operation and Development, Guidelines governing the protection of privacy and transborder flows of personal data (1980, amended in 2013).
[638] Data Protection Convention 1981.
[639] Article 4(1) of the Data Protection Convention.
[640] See on standard-setting by the Council of Europe's Committee of Ministers and Parliamentary Assembly: Nikoltchev &McGonagle 2011, p. 1-3; Nikoltchev &McGonagle 2011, p. 1-3.
[641] Committee of Ministers, Recommendation (85)20 (direct marketing); Committee of Ministers, Recommendation (99)5 (privacy on the Internet), Committee of Ministers, Recommendation (2010)13 (profiling). See for an overview of the Council of Europe data protection texts: <www.coe.int/dataprotection>.
[642] See for instance ECtHR, S. and Marper v. The United Kingdom, No. 30562/04 and 30566/04. 4 December 2008 (citing Recommendation (87)15); ECtHR, Von Hannover v. Germany (I), No. 59320/00, 24 September 2004; ECtHR, Von Hannover v. Germany (II), Nos. 40660/08 and 60641/08, 7 February 2012 (both citing Resolution 1165 (1998) on the right to privacy).
[643] See European Commission 1981; Kuitenbrouwer 2000, p. 44; Platten 1996, p. 17-18; p. 23.
[644] Article 12.3 of the Data Protection Convention allows states to derogate from the prohibition of interfering with cross border data flows, in brief because of the special nature of personal data, or to avoid circumvention of data protection law.

Many stakeholders feared that national authorities would stop the export of personal data to other European countries.[645] This led to action by the European Commission to harmonise data protection law in the EU.[646]

In 1990, the European Commission presented a proposal for a Data Protection Directive.[647] Heated discussions ensued, for instance about the proposal's rules on direct marketing.[648] Business organisations, including the European Direct Marketing Association, started lobbying intensely.[649] Marketers feared that direct mail marketing would only be allowed with the data subject's prior consent. The lobbying paid off. In 1992 the Commission presented an amended proposal, which suggests that direct mail marketing is allowed without prior consent – on an opt-out basis.[650] After the 2012 proposal for a Data Protection Regulation, history repeated itself. Marketers started lobbying heavily, in order to be able to use behavioural targeting on an opt-out basis.[651]

In 1995 the *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* was adopted. This Data Protection Directive has two goals. The first goal is safeguarding the free flow of personal data between member states.[652] Second, the Directive aims to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[653] The wording shows that

---

[645] For example, the French Data Protection Authority had stopped FIAT from exporting personal data from France to Italy in 1989. The transfer was allowed after FIAT made contractual arrangements to safeguard the personal data (Schwartz 2009, p. 11). For more examples of troubles with transborder data flow within the EU see Vassilaki 1993; Stadlen 1976, p. 185-186.

[646] According to Nugter, the European Commission focused mostly on the interests of data controllers, and the European Parliament mostly on the interests of data subjects (Nugter, 1990, p. 29).

[647] European Commission 1990.

[648] See generally about the legislative history of the Data Protection Directive Simitis 1994; Platten 1996; Heisenberg 2005, chapter 3.

[649] Regan 1993, p. 266-267; Heisenberg 2005, p. 62.

[650] See chapter 6, section 2: the Directive sometimes allows processing for direct marketing without consent; namely on the basis of the balancing provision (article 7(f)), which, in short, lays down an opt-out system for direct marketing under certain circumstances.

[651] See chapter 5, section 5.

[652] Article 1(1) of the Data Protection Directive. See González Fuster 2014, p. 130.

[653] Article 1(1) of the Data Protection Directive.

the Directive protects not only privacy rights, but other rights and interests as well. The Data Protection Directive became one of the world's most influential data protection texts.[654]

Data protection law isn't just a European affair.[655] In 1990 the United Nations adopted the Guidelines for the Regulation of Computerized Personal Data Files.[656] These are essentially recommendations to national lawmakers to implement data protection principles. Many non-European countries have passed legislation inspired by the Directive. In July 2013, there were about a 100 countries in the world with a data protection law.[657] The US doesn't have a general data protection law for the private sector, which makes it a lonely exception among developed nations. Recently the Federal Trade Commission and the White House called for privacy regulation for the private sector based on a version of the fair information principles; whether these calls will lead to regulation remains to be seen.[658]

The right to data protection and the right to privacy are increasingly seen as distinct rights. In a 2012 text on the modernisation of the Council of Europe's Data Protection Convention, "[i]t is proposed to refer, in addition to the right to privacy, to the right to the protection of personal data which has acquired an autonomous meaning over the last thirty years."[659] The European Commission's 2012 proposal for a Data Protection Regulation only mentions privacy four times.[660] Article 1 of the proposal provides that the "Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data." The 1995 Directive still mentions privacy in article 1.

---

[654] See Birnhack 2008.
[655] On of the first, possibly the first, versions of the fair information principles was published in the US (United States Department of Health, Education, and Welfare 1973).
[656] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990.
[657] See Greenleaf 2013a; Greenleaf 2013b.
[658] Federal Trade Commission 2012; White House 2012.
[659] Council of Europe, The Consultative Committee Of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ets No. 108) 2012, p. 2. See also González Fuster 2014, p. 92.
[660] The four instances don't include the introduction to the proposal (European Commission proposal for a Data Protection Regulation (2012), p. 1-16). The 1995 Data Protection Directive, which is much shorter, mentions privacy thirteen times. See also González Fuster 2014, p. 242-245.

The EU Charter of Fundamental Rights, adopted in 2000 and legally binding since 2009, contains a separate right to data protection in article 8.[661] This illustrates that data protection has grown into a separate field of law in Europe.[662]

> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

4.2 Overview of the data protection principles

The Data Protection Directive lays down an omnibus regime, which applies to the private sector and the public sector (with exceptions to the latter).[663] The strength of a broadly applicable data protection law with open norms is that the law doesn't leave any gaps. Yet this regulatory approach means that the norms can't be too specific. As

---

[661] See also article 16 of the Treaty on the Functioning of the EU (consolidated version 2012).

[662] As González Fuster 2014 shows, a number of European countries didn't historically see data protection as a privacy-related right (chapter 2 and 3; p. 268). See generally on the "emergence of personal data protection as a fundamental right of the EU" González Fuster 2014.

[663] Some parts of the public sector are outside the scope of the Directive (see article 3(2) and article 13). Some data processing practices in the private sector are also exempted, for purely personal purposes (article 3(2). There are also exemptions for the processing for journalistic purposes (article 9). See on journalistic purposes ECJ, C-73/07, Satamedia, 16 December 2008; CJEU, C-131/12, Google Spain, 13 May 2014.

the European Court of Justice puts it, the Directive's "provisions are necessarily relatively general since it has to be applied to a large number of very different situations."[664]

When applying data protection law, a firm has to go through a number of steps, which often require interpreting rather open norms, such as "fairly", "necessary", and "not excessive."[665] But the complicated nature of data protection law shouldn't be exaggerated. Data protection law gives a relatively objective checklist to assess the fairness of personal data processing. Data protection law can be applied without engaging in discussions about the scope or meaning of the right to privacy, a notoriously slippery concept. Imagine how difficult it would be for firms if the only guidance was: don't infringe on privacy and other fundamental rights when you process personal data.[666]

The core of data protection law can be summarised in nine principles. This study uses Bygrave's taxonomy of eight principles, but adds the transparency principle.[667] Bygrave includes this in the fair and lawful principle. The nine principles are: the fair and lawful processing principle, the transparency principle, the data subject participation and control principle, the purpose limitation principle, the data minimisation principle, the proportionality principle, the data quality principle, the security principle, and the sensitivity principle. There are no clear borders between the different principles, which overlap in different ways. Some principles consist of clusters of other principles. Some principles can be recognised in various provisions within data protection law.[668]

---

[664] ECJ, C-101/01, Lindqvist, 6 November 2003, par. 83. See also ECJ, Joined Cases C−468/10 and C−469/10 (ASNEF), par. 35.
[665] See article 6(1)(a), 6(1)(c), and 6(1)(c) of the Data Protection Directive.
[666] See De Hert & Gutwirth 2006, p. 94. Chapter 9, section 1 returns to the topic of general and specific rules.
[667] Bygrave has presented the taxonomy in Bygrave 2002, chapter 3 and 18, and presented an updated and more concise version in Bygrave 2014, chapter 5. I use a slightly different terminology than Bygrave.
[668] Bygrave 2002, p. 57.

The fair and lawful processing principle is the overarching norm of data protection law. Personal data have to be processed "fairly and lawfully", says the Data protection Directive.[669] The lawfulness requirement is reasonably clear: data processing has to comply with data protection law and other laws. Fairness is more vague. Among other things, it requires transparency.[670] Koops summarises that data protection law aims for "common decency."[671] Section 4 of this chapter returns to the topic of fairness.

This study sees the transparency principle as the most important principle next to the fair and lawful principle (see the next section of this chapter). Data processing must take place in a transparent manner, and secretive data collection isn't allowed (unless an exception applies, for instance for national security).[672] The European Commission proposal for a Data Protection Regulation emphasises the importance of transparency, by adding the transparency requirement to the first data protection principle: "[p]ersonal data must be (…) processed lawfully, fairly and in a transparent manner in relation to the data subject."[673]

The data subject participation and control principle aims to involve the data subject.[674] Involvement of the individual can only be achieved if he or she is aware of the processing. People derive several rights from the data subject participation and control principle. For instance, in some cases firms are only allowed to process personal data after the data subject has given consent. In many other cases, people have the right to object to data processing.[675] Data subjects have the right to obtain information from a firm about whether their data are being processed, and for what purposes.[676] The data subject also has the right to rectify or erase data,[677] and to object to certain types of

---

[669] Article 6(1)(a) of the Data Protection Directive. See Bygrave 2002, p. 58; Bygrave 2014, p. 146.
[670] Recital 38 of the Data Protection Directive. See also Article 29 Working Party 2006, WP 118, p. 9.
[671] Koops 2008, p. 331.
[672] See article 10 and 11 and recital 38 of the Data Protection Directive, and for exceptions article 13.
[673] Article 5(1) (a) of the European Commission proposal for a Data Protection Regulation (2012).
[674] In 2002 Bygrave spoke of the "data subject participation and control" principle; in 2014 he renamed it "data subject influence" principle (Bygrave 2002, p. 63-67; Bygrave 2014, p. 158-163).
[675] Consent: article 7(a), 8(2)(a), 26(1)(a); object: article 14 of the Data Protection Directive. See chapter 6.
[676] Article 12(a) of the Data Protection Directive.
[677] Article 12(b) of the Data Protection Directive.

automated decisions.[678] The influence of the concept of privacy as control over personal information is clear.

According to the purpose limitation principle, personal data must be collected for specified, explicit and legitimate purposes, and must not be further processed for incompatible purposes.[679] The first requirement is sometimes called the purpose specification principle. Personal data may be processed on the basis of the consent of the person concerned or another legal basis. These other legal bases are listed exhaustively, and can only be relied upon if the processing is "necessary."[680] The purpose limitation principle and the requirement for a legal basis to process personal data are discussed in more detail below.[681]

The data minimisation principle prohibits excessive processing in relation to the processing purpose. The principle can be recognised in various provisions. For instance, a firm may not process more personal data than necessary, or store data longer than necessary.[682] Collecting personal data because "you never know, it might come in useful one day" would breach the purpose limitation principle, the data minimisation principle, and the transparency principle.[683] Chapter 9 returns to the data minimisation principle.[684]

The proportionality principle was mainly developed in case law. "One of the most striking developments over the last decade in European data privacy law", notes Bygrave, "is the emergence of a requirement of proportionality as a data protection

---

[678] Article 15 of the Data Protection Directive. See in detail about this provision chapter 9, section 6.
[679] Article 6(b) of the Data protection Directive. The principle could be summarised in the slogan "select before you collect" (Jacobs 2005, p. 1006). See Bygrave 2002, p. 61; Bygrave 2014, p. 153-157.
[680] Article 7 of the Data Protection Directive. See also article 8(2) of the EU Charter of Fundamental Rights.
[681] See section 3 of this chapter (purpose limitation) and chapter 6 (legal basis).
[682] Article 6(1)(c), 6(1)(e) of the Data Protection Directive. See Bygrave 2002, p. 59-61; Bygrave 2014, p. 151-153. See on "necessity" chapter 6, section 1 and 2.
[683] A similar phrase was used (in Dutch) during the legislative history of the Dutch Data Protection Act (Kamerstukken II 1998/99, 25 892, nr. 6, p. 34).
[684] See chapter 9, section 3.

principle in its own right."[685] Proportionality plays two roles in data protection law.[686] First, it's a general principle of data protection law. Second, proportionality is often relevant when applying data protection provisions, for instance when a provision uses the word "necessary" (see chapter 6).[687]

The application of the proportionality principle can be illustrated by the data retention judgment of the European Court of Justice. The Court states that "the principle of proportionality requires that [measures] be appropriate for attaining the legitimate objectives pursued (…) and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives."[688] The Court invalidates the Data Retention Directive because "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of" the right to private life and the right to data protection.[689]

The data quality principle requires an appropriate level of accuracy, completeness, and relevancy of personal data.[690] Firms must take reasonable steps to ensure they erase or rectify inaccurate data. In principle, the data controller must comply if a data subject requests to have incorrect data rectified. The data quality principle aims to reduce the chance that organisations base decisions about people on incorrect data. This corresponds with the fear of powerful organisations with opaque computers in the early 1970s. But the data quality principle remains relevant. Decisions based on incorrect data can have disastrous effects for a data subject.[691]

The security principle requires an appropriate level of security for personal data processing, and confidentiality of the data being processed. Firms that process

---

[685] Bygrave 2014, p. 147. In 2002 Bygrave didn't list the proportionality principle, but listed the "disclosure limitation principle" instead (Bygrave 2002, p. 67).
[686] Kuner 2008, p. 1616-1617.
[687] See chapter 6, section 1 and 2 (on "necessary" in article 7 of the Data Protection Directive), and chapter 9, section 3 on data minimisation and proportionality.
[688] CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 46.
[689] CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 69.
[690] Bygrave 2002, p. 62; Bygrave 2014, p. 163-164; article 6(1)(d) of the Data Protection Directive. The data quality principle falls outside the scope of the thesis.
[691] See for instance ECtHR, Romet v. Netherlands, No. 7094/06, 14 February 2012.

personal data must protect the data against unauthorised disclosure or access, and other unlawful forms of processing.[692]

The sensitivity principle refers to the stricter regime for "special categories" of personal data. Examples are data revealing racial or ethnic origin, religious beliefs, and data concerning health or sex life.[693] Processing such special categories of data is in principle prohibited, unless a legal exception applies such as medical necessity.[694] A member state can choose to allow data subjects to override this prohibition by giving their "explicit consent."[695] Apart from the special categories of data, the nature of data is relevant when applying data protection law. More sensitive data call for stricter application of the rules.

Additional rules

Next to the core data protection principles, Bygrave distinguishes a second group of rules, which mainly concern enforcement of the principles.[696] For instance, compliance with data protection law is subject to control by independent Data Protection Authorities. This requirement is laid down in the EU Charter of Fundamental Rights.[697]

The Data Protection Directive distinguishes "data controllers" from "data processors." The data controller is the party that determines the purposes and means of the personal data processing.[698] The controller is responsible for compliance.[699] A data

---

[692] Bygrave 2002, p. 67; Bygrave 2014, p. 164-165. See article 16 and 17 of the Data Protection Directive. See also article 4, and recitals 6, 20, 24 and 25 e-Privacy Directive. A definition of "network and information security" can be found in art. 4(c) of the ENISA Regulation (EC) 460/2004. See on communications security Arnbak 2013a.
[693] Article 8 of the Data Protection Directive. Bygrave 2002, p. 68; see also 131-132.
[694] Article 8(c) of the Data protection Directive.
[695] Article 8(2)(a) of the Data Protection Directive.
[696] Bygrave 2002, chapter 4, p. 70-83.
[697] Article 8(3) of the EU Charter of Fundamental Rights. Data Protection Authorities (DPAs) go under various names in the member states. For instance, in the United Kingdom the DPA is called the Information Commissioner's Office, and in France the Commission Nationale de l'Informatique et des Libertés (CNIL) [National Commission on Informatics and Liberty].
[698] Article 2(d) of the Data Protection Directive. The Directive also defines "third parties" and "recipients" (article 2(f) and 2(g)). This study doesn't discuss such parties.
[699] Article 6(2)(b) and 23(1) of the Data Protection Directive

processor is a party that processes personal data on behalf of the controller.[700] The distinction between controllers and processors is difficult to make sometimes, and the distinction's usefulness has been questioned.[701] Nevertheless, the European Commission proposal for a Data Protection Regulation keeps the distinction.[702] The difficulty is apparent with behavioural targeting, because many parties can be involved in delivering an ad. The Working Party says ad networks and website publishers are often joint data controllers, as they jointly determine the purposes and means of the processing. For instance, the website publisher allows the ad network to place cookies through its site. The Working Party says a website publisher can't escape its responsibilities by saying that it doesn't know what ad networks do through its website.[703] For ease of reading, this study often refers to firms, without specifying whether a firm is the controller or the processor.

In principle, the Data Protection Directive prohibits transferring personal data to countries outside the EU, if those third countries don't offer an adequate level of protection to personal data.[704] The data subject can override this prohibition by giving consent for a transfer.[705] For the US, which doesn't have the status of a country with "adequate" protection, a special "Safe Harbor" arrangement is in place. In short, firms from the US from certain sectors are deemed to offer an adequate level of protection if they agree to comply with the data protection principles.[706]

---

[700] Article 1(e) of the Data Protection Directive. The processor has mainly responsibilities regarding confidentiality (article 16).
[701] See on the roles of processors and controllers Article 29 Working Party 2010, WP 169; Van Alsenoy 2012. For criticism on the distinction Traung 2012; Purtova 2011, p. 171-174.
[702] Article 4(5) and 4(6) of the European Commission proposal for a Data Protection Regulation (2012).
[703] Article 29 Working Party 2010, WP 171, p. 11. The distinction between controllers and processors falls outside the scope of this study.
[704] Article 25 and 26 of the Data Protection Directive.
[705] Article 26(1)(a) of the Data Protection Directive.
[706] See the website about the Safe Harbor program <www.export.gov/Safeharbor>. See on the negotiations that lead to the agreement Heisenberg 2005, chapter 4. The Safe Harbor program was always controversial, but the criticism grew after the Snowden revelations about international surveillance by US Intelligence Agencies in 2013 (see LIBE Committee 2014).

The Data Protection Directive also contains rules to establish whether firms from outside the EU have to comply with the EU rules.[707] The two main rules regarding territoriality can be summarised as follows. First, European data protection law applies when processing is carried out in the context of the activities of an establishment of a firm on EU territory.[708] Second, the law applies when the firm is not established in the EU, but uses equipment situated on EU territory for personal data processing.[709] Several of the largest firms that use behavioural targeting are formally established in Europe, such as Facebook and Apple (Ireland), and Microsoft (Luxemburg). Many other non-European firms also use equipment, such as data centres, in Europe. The Working Party says, in short, that European data protection law applies to any firm that uses tracking technologies on a device in Europe, because in such cases the firm makes use of equipment (the user's device) in Europe.[710] The territorial scope of data protection law has been analysed extensively elsewhere and falls outside the scope of this study.[711] For this study the conclusion will suffice that EU data protection law often applies to firms that are usually regarded as non-European firms.

Data Protection Regulation proposal

After a two-year consultation period, the European Commission presented its proposal for a Data Protection Regulation in January 2012. Many scholars and civil rights organisations welcomed the proposal.[712] Others were less enthusiastic – one US

---

[707] Article 4 of the Data Protection Directive. The Directive as such doesn't apply to firms outside the EU; rather the national provisions based on the Directive apply.
[708] Article 4(1)(a) of the Data Protection Directive. In the Google Spain case, the European Court of Justice applies this provision. In short, EU data protection law applies when a search engine operator has a subsidiary in a member state, and that subsidiary sells and promotes advertising space offered by the search engine (CJEU, C-131/12, Google Spain, 13 May 2014, dictum, 2). Regarding the territorial scope the Court follows the Advocate General, who based his reasoning, in part, on Article 29 Working Party 2008, WP 148, p. 9-12.
[709] Article 4(1)(c) of the Data Protection Directive.
[710] Article 29 Working Party 2008, WP 148, p. 9-12.
[711] On the extra-territorial reach of data protection law, see Article 29 Working Party 2010, WP 179; Moerel 2011, chapter 1-4; Kuner 2010; Kuner 2010a; Piltz 2013. The e-Privacy Directive potentioally has an even broader territorial scope than the Data Protection Directive (see Kuner 2010, p. 191-192).
[712] See for instance De Hert & Papakonstantinou 2012; EDRi (European Digital Rights) 2012. See for overview articles on the 2012 proposal Hornung 2012; Kuner 2012a; Van Der Sloot 2012a; Zanfir 2014.

scholar spoke of "more crap from the EU"[713] While based on the same principles as the Directive, the Regulation would bring significant changes. For instance, a regulation has direct effect. Unlike a directive, a regulation doesn't have to be implemented in the national laws of the member states.[714] Hence, a regulation should lead to a more harmonised regime in Europe. Less divergence between national rules should make it easier to do cross-border business.

With 91 provisions, the proposed Regulation is much longer than the 1995 Directive (34 provisions). There are new requirements for data controllers, such as the obligation to implement measures to ensure and demonstrate compliance.[715] In some circumstances, data controllers must undertake a data protection impact assessment before they start processing.[716] But the proposal also brings advantages for firms, such as the abolishment of the requirement to notify Data Protection Authorities of data processing practices.[717] The European Commission estimates the regulation could lead to savings for businesses of around 2.3 billion Euros per year.[718]

The proposal emphasises the ideal of data subject control. Pursuant to the preamble, "[i]ndividuals should have control of their own personal data."[719] For instance, the proposal requires consent to be "explicit" and sets out more detailed rules regarding transparency.[720] The rights to request erasure and to withdraw consent are

---

[713] Yakowitz 2012.
[714] Article 288 of the Treaty on the Functioning of the EU (consolidated version 2012).
[715] Chapter IV, section 1 of the European Commission proposal for a Data Protection Regulation (2012).
[716] Article 33 of the European Commission proposal for a Data Protection Regulation (2012). See on privacy and data protection impact assessments Kloza 2014, and the PIAF project (Privacy Impact Assessment Framework for data protection and privacy rights, <http://piafproject.eu>).
[717] European Commission proposal for a Data Protection Regulation (2012), p. 10 and article 28.
[718] Impact Assessment for the proposal for a Data Protection Regulation (2012), p. 3.
[719] Recital 6 (and p. 2) of the European Commission proposal for a Data Protection Regulation (2012). See also Impact Assessment for the proposal for a Data Protection Regulation (2012), p. 41.
[720] Article 4(8) and 7 of the European Commission proposal for a Data Protection Regulation (2012). See for more details chapter 6, section 3, and chapter 8, section 3.

emphasised.[721] A right to data portability is introduced, which should make it easier for people to transfer their data from one service provider to another.[722]

Enforcement and the right to redress are strengthened in the European Commission proposal. In certain circumstances, Data Protection Authorities can impose fines of up to one million Euros or, in the case of an enterprise, up to 2% of its annual worldwide turnover.[723] The European Parliament has proposed fines of up to 5%.[724] Another novelty is that organisations that aim to protect data subject rights can sue a data controller that breaches data protection law.[725] The proposed Regulation also applies to the processing of personal data of people residing in the EU by a non-European firm, if the processing relates to "the monitoring of their behaviour."[726] This would apply to behavioural targeting.

The proposal has led to much debate and much lobbying.[727] Members of the European Parliament have proposed 3999 amendments.[728] In March 2014, the European Parliament adopted a compromise text ("LIBE Compromise"), which the Parliament's LIBE Committee prepared on the basis of the 3999 amendments by the members of parliament. The rules for behavioural targeting in the LIBE Compromise are less strict than those in the European Commission proposal.[729] At the time of writing, the proposed Regulation is still being discussed in Brussels. It's unclear whether the

---

[721] Article 17 of the European Commission proposal for a Data Protection Regulation (2012) had the somewhat misleading title "the right to be forgotten." See on a right to be forgotten Ausloos et al. 2012 (mostly positive); Van Hoboken 2013 (more critical); Mayer-Schönberger 2009 (US focused). See also CJEU, C-131/12, Google Spain, 13 May 2014, and on that case Kulk & Zuiderveen Borgesius 2014.
[722] Article 18 and recital 55 of the European Commission proposal for a Data Protection Regulation (2012); article 15(2) of the LIBE Compromise, proposal for a Data Protection Regulation (2013).
[723] Article 79 of the European Commission proposal for a Data Protection Regulation (2012).
[724] Article 70(2a)(c) of the LIBE Compromise, proposal for a Data Protection Regulation (2013).
[725] Article 76(1) of the European Commission proposal for a Data Protection Regulation (2012).
[726] Article 3; recital 20 and 21 of the European Commission proposal for a Data Protection Regulation (2012). See also Impact Assessment for the proposal for a Data Protection Regulation (2012), p. 41-42.
[727] The website LobbyPlag shows which amendments by members of the European Parliament were copied literally from lobbyists (<http://lobbyplag.eu>). One member tabled over 150 amendments to weaken the proposal, many of which were copied from lobbyists. He later said he wasn't aware that his assistant submitted the amendments (See Nielsen 2013; Brems 2013).
[728] See LIBE Committee, Documents relating to procedure 2012/011(COD).
[729] See chapter 5, section 5; chapter 6, (the end of) section 3.

proposal will be adopted. The most optimistic view seems to be that the Regulation could be adopted in 2015.[730]

4.3 Transparency

A basic tenet of data protection law is that data processing should take place in a transparent manner. Following De Hert & Gutwirth, the legal right to privacy can be characterised as an "opacity tool" and data protection law as a "transparency tool."[731] Opacity tools aim "to guarantee non-interference in individual matters, or the opacity of the individual."[732] Transparency tools aim "to make the powerful transparent and accountable: they allow us 'to watch the watchdogs'"[733]

Article 8 of the European Convention on Human Rights prohibits intrusions into the private sphere. This prohibition is not absolute; privacy must often be balanced against other interests, such as the rights of others or the prevention of crime. The structure of article 8 of the Convention is as follows. In principle there's a prohibition on privacy infringements (paragraph 1): "There shall be no interference by a public authority with the exercise of this right (…)." But exceptions to this prohibition are possible under strictly defined conditions, for instance in the interests of national security, or to protect the rights and freedoms of others (paragraph 2). De Hert & Gutwirth characterise the legal right to private life as a "no, unless" rule.[734] The right aims to allow the individual to remain shielded, or to remain opaque: it's an opacity tool. Their characterisation of the legal right to privacy thus appears to be related to privacy as limited access.[735]

Data protection law takes another approach than the legal right to privacy, according to De Hert & Gutwirth. In principle, data protection law allows data processing, if the

---

[730] See European Council 2014, p. 2.
[731] De Hert & Gutwirth 2006; De Hert & Gutwirth 2008. See chapter 1, section 1, and chapter 9, section 2.
[732] De Hert & Gutwirth 2006, p. 66.
[733] De Hert & Gutwirth 2008, p. 277. See also Bennett 2011a, p. 491.
[734] De Hert & Gutwirth 2008, p. 291.
[735] See on privacy as limited access: chapter 3, section 1.

data controller complies with a number of requirements. Data protection law is mainly a regime of "yes, but."[736] Data protection law aims to manage rather than to stop data flows. "Data protection regulation does not protect us from data processing, but from unlawful and/or disproportionate data processing."[737] As Bygrave puts it, data protection law "usually posts the warning 'Proceed with care'; it rarely orders 'Stop!'"[738] One of data protection law's main tools to foster fairness is the requirement that data processing happens transparently. Data protection law aims to prevent abuse of information asymmetry.[739] "No openness, no legitimacy," says Gutwirth.[740] Hence: a transparency tool.[741]

The Data Protection Directive's transparency requirements aren't a new invention. One of the first texts listing principles for fair information processing is a 1973 report from the US. The first of its five principles states: "[t]here must be no personal-data record-keeping systems whose very existence is secret." The second principle adds that "[t]here must be a way for an individual to find out what information about him is in a record and how it is used."[742] The OECD Data Protection Guidelines say that personal data "should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[743] The Annex to the 1980 Guidelines adds that this provision "is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent

---

[736] De Hert & Gutwirth 2008, p. 291.
[737] Gutwirth & De Hert 2009, p. 3. González Fuster & Gutwirth call the transparency tool interpretation of data protection law a "permissive notion", which they contrast with a "prohibitive notion" (González Fuster & Gutwirth 2013, p. 532). The permissive notion can also be recognised in Blume 2012, p. 28; Blok 2002, p. 326.
[738] Bygrave 2014, p. 122.
[739] The phrase "abuse of information asymmetry" was used in the privacy context by OrwellUpgraded 2013.
[740] Gutwirth 2002, p. 96.
[741] The analysis of De Hert & Gutwirth 2006 is widely cited. But there's also criticism; see Verbruggen 2006; Tzanou 2012; Tzanou 2013.
[742] United States Department of Health, Education, and Welfare 1973, p. 41.
[743] Collection Limitation Principle. This article 7 is phrased the same in 1980 and the 2013 version of the OECD Data Protection Guidelines.

of the data subject is as a rule essential, knowledge being the minimum requirement."[744]

Borrowing from Van Alsenoy et al., five justifications for data protection law's transparency requirements can be distinguished. First, fairness logically requires transparency: "even if one doesn't have a real say in the matter, an individual should, in principle, at least be put 'on notice' when his personal data is being processed."[745] Second, transparency is necessary to enable data subjects to exercise their rights, such as access, correction and deletion rights, and the right to opt out of data processing.[746] Third, the requirement to disclose information, for instance in a privacy policy, can nudge a firm towards reviewing its data processing practices.[747] If a firm wants to explain its data processing practices, it has to know about them.[748] Fourth, transparency fosters accountability. "If drafted properly, a privacy notice enables scrutiny of a company's data collection and use practices."[749] Transparency could also help Data Protection Authorities to obtain an overview of types and risks of processing.[750] Fifth, the transparency requirements aim to reduce the information asymmetry between data subjects and data controllers, "as a first, albeit relatively modest, step towards 'leveling the playing field' between data subjects and controllers in terms of the knowledge acquired through processing."[751] Chapter 7 shows that from an economic perspective, it's not only in the interest of the individual, but also in the public interest to reduce information asymmetry.[752]

---

[744] Annex to the Recommendation of the Council of 23rd September 1980, par. 52.
[745] Van Alsenoy et al. 2013, p. 2. See on transparency also Zarsky 2013, p. 1530-1553. US scholar Calo mentions another reason for regulators to focus on transparency requirements that should enable people to make choices: "regulators use notice to avoid having to actually regulate" (Calo 2013a, p. 795).
[746] Van Alsenoy et al. 2013, p. 2-3.
[747] Privacy policies are also called privacy notices or privacy statements.
[748] Van Alsenoy et al. 2013, p. 3. See also Solove 2013, p. 1900.
[749] Van Alsenoy et al. 2013, p. 3. See also Bennett 2011a.
[750] The obligation to notify the Data Protection Authority of (certain) processing operations can also be seen in this light (article 18 of the Data protection Directive). This obligation is abolished in the European Commission proposal for a Data Protection Regulation (2012), p. 10.
[751] Van Alsenoy et al. 2013, p. 2.
[752] Information asymmetry is a form of market failure. See chapter 7, section 3.

The Directive's article 10 and 11 concern "information to be given to the data subject." A firm must provide at least information regarding its identity and the processing purposes.[753] The firm must provide more information when necessary to guarantee fair processing. The Directive gives examples of information that could be needed to ensure fairness: the categories of data concerned, the recipients or categories of recipients, and information about the right to access and to rectify data.[754]

Article 10 applies when a firm collects data from the data subject; article 11 applies "where the data have not been obtained from the data subject." In the case of data collection for behavioural targeting on websites, the Working Party says that the website publisher is usually a joint data controller and must inform the data subject.[755] When article 10 or 11 applies can be difficult to determine, but the information that a firm must provide is the same anyway. The main difference is the moment at which the information must be given.

If article 11 applies, the firm must give the information "at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed."[756] If tracking by ad networks were seen as not obtaining data from the data subject, article 11 would apply. Hence, the ad network would have to inform the data subject when it collects the data (at the time of "recording"). Or the ad network would have to inform the data subject when it allows advertisers to target people with ads, which should probably be seen as data disclosure under data protection law.[757] However, chapter 6 shows that consent is almost always required for personal data processing for behavioural targeting. If a firm seeks consent, article 10 applies, as the firm collects the data directly from the data subject.

---

[753] Büllesbach 2010, comment on article 10, p. 68.
[754] Article 10 and 11 of the data Protection Directive. The Council of Europe has given guidance for the transparency requirements for profiling (article 4 of the Profiling Recommendation (2010)13).
[755] Article 29 Working Party 2010, WP 171, p. 11.
[756] Article 11(1) of the data Protection Directive.
[757] See chapter 6, section 2 (and chapter 2, section 6).

There are some exceptions to the transparency requirement, which are discussed in chapter 8.[758]

To slightly rephrase Verhelst, a privacy policy is an instrument that a data controller can use to comply with its obligation to provide information pursuant to article 10 and 11 of the Data Protection Directive.[759] Privacy policies must be distinguished from consent requests. The Directive always requires firms to be transparent about personal data processing. Even if a firm doesn't want to rely on consent as a legal basis for processing personal data, data protection law requires transparency.

Purpose limitation principle

The purpose limitation principle also fosters transparency. A firm must specify the collection purposes, and personal data must not be "further processed in a way incompatible with those purposes."[760] If data subjects consent to their data being used for one goal, the purpose limitation principle should ensure that they don't have to worry that the data will be used for unrelated goals. Informed consent would be worthless if firms were free to use personal data for new purposes at will. To establish whether a new purpose is "incompatible", the collection context should be taken into account.[761]

But the purpose limitation principle isn't as strict as it might seem. First, the processing purposes must be "specified", but the law allows a firm to ask consent for many purposes, as long as these purposes are clearly described. One English author summarises: "[a]t the heart of data protection legislation is the concept that it is

---

[758] See chapter 8, section 2.
[759] His definition is as follows: "a privacy statement is an instrument which the data controller can use to comply with his obligation to provide information pursuant to Articles 33 and 34 Wbp [Dutch Data Protection Act]. The data controller can formalise the content and therefore the implementation of the obligation to provide information by means of this privacy statement" (Verhelst 2012, p. 224).
[760] Article 6(1)(b) of the Data Protection Directive. The European Commission proposal for the Data Protection Regulation (2012) appears to soften the purpose limitation principle (article 6.4).
[761] See Bygrave 2014, p. 157. See generally on privacy as contextual integrity Nissenbaum 2010. The European Court of Human Rights also takes the collection context into account. See e.g. ECtHR, Niemietz v. Germany, No. 13710/88, 16 December 1992, par. 28; ECtHR, Von Hannover v. Germany (I), No. 59320/00, 24 September 2004, par. 68; ECtHR, S. and Marper v. The United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 67.

possible to do almost anything with personal data if the relevant consent to the relevant purpose has been obtained from the relevant individual."[762] This seems exaggerated, as consent only concerns the legal basis for processing.[763] The data subject can't waive data protection law's provisions. Nevertheless, cunningly phrased consent requests can reduce the value of the purpose limitation principle. And many people might click "yes" anyway.[764]

Second, firms have some leeway because they're allowed to process personal data for a new purpose if it's "not incompatible" with the collection purpose. While the interpretation of the phrase "not incompatible" varies by member state, it's clear that purposes that are fully unexpected for the data subject aren't allowed.[765]

Third, the Directive softens the purpose limitation principle, because "[f]urther processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that member states provide appropriate safeguards."[766] Firms could try to claim that predictive modelling for behavioural targeting is a form of statistical analysis, which can be based on this exception.[767] Nevertheless, although the purpose limitation principle is softened somewhat, it could still protect people against unexpected uses of their data.

Other data protection provisions also aim for transparency. For example, in many circumstances firms must obtain the data subject's consent for processing. This obligation should foster transparency, as the data subject is alerted to the data processing when the firm asks for consent. Furthermore, data subjects have the right

---

[762] Carey 2002, p. 37.
[763] Moreover, sometimes valid consent can't be obtained, because it wouldn't be voluntary. See chapter 6, section 3 and 4, and chapter 8, section 3 and 5.
[764] See chapter 7.
[765] Article 29 Working Party 2013, WP 203.
[766] Article 6(1)(b) of the Data Protection Directive (capitalisation adapted). See on statistical data also Council of Europe, Committee of Ministers (1997), Statistical Purposes Recommendation Rec(97)18; Ploem 2004, chapter 3.
[767] Firms would still need to comply with data protection law when processing personal data, for instance when collecting personal data (phase 1).

to hear from a firm what data of theirs it processes, for what purposes, and whether and to whom the data are disclosed.[768]

4.4 Fairness

The main requirement of data protection law is that data processing happens "fairly and lawfully."[769] Lawfully means that firms have to comply with data protection law and other laws. But what does fairness mean? The Data Protection Directive's preamble offers some insight. According to the preamble, fairness requires transparency: "if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection."[770] Furthermore, data processing should serve mankind, people's well-being, and social and economic progress.

> [D]ata-processing systems are designed to serve man; (…) they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals.[771]

---

[768] See regarding access, erasure and opt-out rights article 12 and 14 of the Data Protection Directive, and regarding access rights also article 8(2) of the EU Charter of Fundamental Rights.
[769] Article 6(1)(a) of the Data Protection Directive.
[770] Recital 38 of the Data Protection Directive. See also recital 28 of the Data Protection Directive, and European Agency for Fundamental Rights 2014, p. 76-77.
[771] Recital 2 of the data Protection Directive (punctuation adapted). Recital 2 of the European Commission proposal for a Data Protection Regulation (2012) says roughly the same. The text of these recitals resembles article 1 of the French Data Protection Act: "Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties."

It's hard to disagree with this, but it might be difficult to operationalise in practice. According to Bygrave, fairness implies that "data controllers must take account of the interests and reasonable expectations of data subjects."[772] He adds that fairness, at a minimum, requires attention to proportionality. Data processing shouldn't have a disproportionate impact on the data subject. Bygrave says fairness also implies that a firm shouldn't pressure people too much into disclosing data, and shouldn't abuse monopoly-like situations.[773] As noted, fairness also logically requires transparency.

Data protection law's fairness principle can be seen as a "safety net" under the more specific requirements.[774] Usually complying with the data protection provisions should ensure that data processing happens fairly. Data protection law could be summarised as one big detailed fairness test. But the lawmaker can never foresee every situation. On rare occasions data processing that complies with all the other data protection provisions may still be illegal because it doesn't comply with the fairness requirement.[775]

For the interpretation of fairness in commercial settings such as behavioural targeting, inspiration can be drawn from European consumer law.[776] Unfair commercial practices are prohibited.[777] Under the Unfair Commercial Practices Directive, a practice is unfair when it's contrary to the requirements of professional diligence, and it's likely to distort a consumer's economic behaviour.[778] The Directive includes a list of commercial practices that are always regarded as unfair.[779] For instance, the presentation of rights given to consumers in law as a distinctive feature of the trader's offer is not allowed.[780] Advertorials that aren't clearly identified as such are

---

[772] Bygrave 2002, p. 58.
[773] Bygrave 2002, p. 58-59; p. 334-337; Bygrave 2014, p. 146-147.
[774] Korff 2005, p. 37.
[775] Korff 2005, p. 37; See also Rouvroy & Poullet 2009, p. 73. See for criticism on the vagueness of the fair and lawful requirement Traung 2012, p. 40.
[776] See Article 29 Working Party 2014, WP 217, p. 44.
[777] Article 5(1) of the Unfair Commercial Practices Directive.
[778] Article 5(2) of the Unfair Commercial Practices Directive. See about the concept of unfairness in that directive Collins 2005.
[779] Article 5(1)(5) of the Unfair Commercial Practices Directive.
[780] Annex 1(10) of the Unfair Commercial Practices Directive.

prohibited.[781] It's also prohibited to describe a product as "free", if the consumer has to pay anything other than the unavoidable cost of responding to the offer and the delivery costs of the item.[782] Such requirements can be applied by analogy to consent requests for personal data processing.

Standard contract terms are unfair when they cause a significant imbalance between the rights of a consumer and a firm. In the words of the Unfair Contract Terms Directive:

> A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.[783]

Fairness and good faith have also been discussed in the context of European contract law.[784] The Draft Common Frame of Reference for European Contract Law (DCFR) is a text prepared by academics, which lays down principles, definitions, and model rules for European contract law.[785] The DCFR says: "[t]he expression 'good faith and fair dealing' refers to a standard of conduct characterised by honesty, openness and consideration for the interests of the other party to the transaction or relationship in question."[786] The European Commission proposal for a Common European Sales law

---

[781] Annex 1(11) of the Unfair Commercial Practices Directive.
[782] Annex 1(20) of the Unfair Commercial Practices Directive. See about this prohibition CJEU, C-428/11, 18 October 2012, Purely Creative. See also European Commission 2014a (about apps and games).
[783] Article 3(1) of the Unfair Contract Terms Directive.
[784] For international contract law, see article 1.7 of the UNIDROIT principles. "Each party must act in accordance with good faith and fair dealing in international trade." See also article 7(1) of the United Nations Convention on Contracts for the International Sale of Goods, which says regard is to be had to the observance of good faith when interpreting the Convention.
[785] The Draft Common Frame of Reference was prepared by the Study Group on a European Civil Code (<www.sgecc.net>) and the European Research Group on Existing EC Private Law (<www.acquis-group.jura.uni-osnabrueck.de>).
[786] Article I-1:103 of the Draft Common Frame of Reference; Principles, Definitions and Model Rules of European Private Law. The Principles of European Contract Law (PECL) contain similar provisions. The PECL require

requires parties to act in accordance with good faith and fair dealing, which is defined almost identically as in the DCFR.[787]

The DCFR also provides rules to assess the fairness of standard terms (that haven't been individually negotiated) in business to consumer contracts. For instance, a standard term is unfair "if it is supplied by the business and if it significantly disadvantages the consumer, contrary to good faith and fair dealing."[788] The DCFR adds that a standard term that isn't drafted in plain, intelligible language may on that ground alone be considered unfair.[789] The good faith requirement in European contract law provides a tool for judges to invalidate unfair contracts. National legal systems in Europe offer judges comparable possibilities.[790] The fairness requirement in data protection law could serve a similar function.

4.5 Protecting and empowering the individual

Law is messy.[791] This also applies to data protection law. The Data Protection Directive is a compromise text that combines elements from earlier national data protection laws in Europe.[792] As is often the case with law, data protection law aims to strike a balance between conflicting interests, and embodies inherent tensions.[793]

For instance, data protection law aims to protect fundamental rights and to foster the internal market at the same time. The titles of the Data Protection Directive and the European Commission proposal for a Regulation reflect this. Both give rules "on the

---

parties to "act in accordance with good faith and fair dealing." A standard term is unfair "if, contrary to the requirements of good faith and fair dealing, it causes a significant imbalance in the parties' rights and obligations" (article 1:201(1) and Article 4:110(1)).

[787] European Commission 2011 (proposal Common European Sales Law), article 2(b).

[788] Article II. – 9:403 of the Draft Common Frame of Reference; Principles, Definitions and Model Rules of European Private Law.

[789] Article II 9:402(1) requires standard contract terms to be "drafted and communicated in plain, intelligible language." (Draft Common Frame of Reference; Principles, Definitions and Model Rules of European Private Law).

[790] Most national legal systems in Europe also have a good faith clause or something similar (Hesselink 2011; Korff 2005, p. 37).

[791] The phrase is used by, among others, Hesselink 2009, p. 28.

[792] Simitis 1994; González Fuster 2014, p. 126.

[793] Bygrave 2002, p. 86; Blume 2012.

protection of individuals with regard to the processing of personal data and on the free movement of such data."[794] Business would benefit from a free flow of personal data within the EU.[795]

Data protection law also aims to balance the interests of data controllers and data subjects.[796] The law aims to protect the data subject's rights and to take the data controllers' interests into account. The law accepts that processing can be useful and necessary. For example, the state is frequently permitted to process personal data without the data subject's consent. Firms are often allowed to process personal data without consent as well.[797]

Rules that aim for data subject control

Another tension is between protection and empowerment of the data subject. Data protection law aims to strike a balance between protecting and empowering people.[798] On the one hand, data protection law aims to empower the data subject. The data subject participation and control principle plays an important role in European data protection law. "A core principle of data protection law," says Bygrave, "is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organizations."[799] Data protection law is deeply influenced by the privacy as control perspective and the concept of informational self-determination.[800] Data protection law relies partly on procedural

---

[794] The 1995 Directive is an internal market directive, as it's based on the old article 95 of the Treaty establishing the European Community, which corresponds to article 114 of the Treaty on the Functioning of the EU (consolidated version 2012). The 2012 proposal is based on article 16 of the Treaty on the Functioning of the EU (consolidated version 2012).

[795] Other international data protection texts also have the dual goal of aiming for fair data processing and the free movement of personal data over borders. See e.g. the Council of Europe Data Protection Convention and the OECD Data Protection Guidelines. The Council of Europe approaches the free flow of information over boarders in the light of article 10 of the European Convention on Human Rights (see Kranenborg 2007, p. 67).

[796] Bonner & Chiasson 2005 suggest the OECD Data Protection Guidelines mainly aim to help firms and other data controllers.

[797] See the legal bases for data processing (article 7(b) and 7(f)) that are discussed in chapter 6.

[798] Blume 2012 highlights this as well, and speaks of "inherent contradictions" in data protection law.

[799] Bygrave 2002, p. 63.

[800] Mayer-Schönberger 1997, p. 232. See on informational self-determination chapter 3, section 1.

safeguards. The idea is that fair procedures regarding data processing should lead to fair outcomes.[801]

Rules that aim for data subject control can be roughly divided into two groups. First, there are rules that give the data subject a choice to allow processing or not. In some cases, firms are only allowed to process personal data after the data subject has given consent.[802] In other cases, firms are permitted to process personal data without consent, but people have a right to object on compelling legitimate grounds. This is a relative right to object. If the objection is justified, the firm must stop the processing. In the case of direct marketing, the data subject has an absolute right to object: to opt out.[803] People can also consent to the export of their data to a country without adequate legal protection of personal data. This way, a data subject can override the in-principle prohibition of transferring personal to a country outside the EU that doesn't offer "an adequate level of protection."[804] (Chapter 6 discusses the role of informed consent in the legal regime for behavioural targeting in detail.) Data protection law's transparency requirements should help data subjects to excersice their rights.[805]

A second set of rules that aim for data subject control grants the data subject rights. For instance, people have the right to access their data. People also have the right to obtain communication of data that are being processed, and of any available information regarding the source of the data. Furthermore, people have the right to obtain information regarding processing purposes, the categories of data concerned, and the recipients to whom the data are disclosed. People can also rectify, erase or block data, if the processing doesn't comply with the Directive's provisions, for

---

[801] Bennett 1992, p. 112; Blok 2002, p. 248-251. See for an analysis of the rights of the data subject in the context of direct marketing Korff 2005, chapter 5.
[802] Article 7(a), 8(a), 26(a) of the Data Protection Directive.
[803] Article 14 of the Data Protection Directive.
[804] Article 26(a) of the Data Protection Directive.
[805] See section 3 of this chapter on the transparency principle, chapter 7, section 3 and 4 for a critique, and chapter 8, section 2 for suggestions to improve transparency.

instance when data are incomplete or inaccurate.[806] And if a firm breaches their data protection rights, people have the right to go to court. The Directive makes the data processor liable in case something goes wrong,[807] and gives data subjects rights that they can enforce.[808] Essentially, the Directive assigns rights and liabilities here.[809]

Rules that aim for data subject protection

On the other hand, many aspects of data protection law aim to protect, rather than to empower, the data subject. First, the mere existence of data protection law could be said to protect the data subject. Data protection law limits what firms can legally do with personal data. Furthermore, the data subject can't make deviating arrangements with a firm; a contract stating that data protection law doesn't apply wouldn't be enforceable.

Another example of a rule that aims to protect the individual, is the obligation for firms to secure the personal data they process.[810] This security principle protects the data subject. For instance, badly secured data could lead to data breaches, which could negatively affect the data subject. The data minimisation is another important requirement that aims to protect the individual.[811] One of the goals of minimising the amount of data processed is to mitigate risks. If fewer data are collected and stored, there are fewer data that can fall into the wrong hands. Another example of how data protection law aims to protect people is the existence of independent Data Protection Authorities that oversee compliance with the rules, as required by the EU Charter of Fundamental Rights.[812]

---

[806] Article 12(a) and 12(b) of the Data Protection Directive. See also article 8(2) of the EU Charter of Fundamental Rights.
[807] Article 23(1) of the Data Protection Directive.
[808] Article 22 of the Data Protection Directive. People rarely go to court for data protection cases. See chapter 8, section 1.
[809] See chapter 1, section 4; Baldwin et al. 2012, chapter 7.
[810] Article 17(1) of the Data Protection Directive.
[811] Article 6(1)(c) and 6(1)(e) of the Data Protection Directive.
[812] Chapter 9 returns to the topic of rules that aim to protect the data subject.

This study distinguishes protection and empowerment rules in order to structure the discussion, but it's not suggested that there's a formal legal distinction. There are no hard lines between rules that aim to protect and to empower the data subject. Some rules have a dual function. For instance, data subjects can't contract away their right to access. This limits the data subject's contractual freedom.[813] But at the same time, the prohibition of waiving one's access rights could be said to foster individual control over personal data. Data subjects would have less control over their data if they could waive their access rights. This study uses rules that aim for *data subject control* and rules that aim for *empowerment* roughly interchangeably.[814]

4.6 Conclusion

This chapter introduced data protection law for the purposes of this study. The key aim of data protection law is ensuring that personal data processing happens fairly and transparently. Data protection law grants people whose data are being processed rights, and imposes obligations on parties that process personal data. Personal data must be processed for specified purposes and on the basis of the consent of the person concerned or another legitimate basis provided by law. Independent Data Protection Authorities oversee compliance with the rules. Data protection law applies when "personal data" are processed. Whether data protection law applies to behavioural targeting is discussed in the next chapter.

Data protection law aims to strike a balance between protecting and empowering the data subject. On the one hand, data protection law aims to empower the data subject by fostering individual control over personal data. On the other hand, data protection law contains many safeguards that the individual can't waive. These safeguards are

---

[813] See in more detail on limiting contractual freedom chapter 6, section 5 and 6; chapter 9, section 2.
[814] However, chapter 9, section 2, argues that protective rules, which limit people's contractual freedom, can sometimes help to ensure real empowerment.

mainly aimed at protecting rather than empowering the individual. The tension between protection and empowerment is a recurring theme in this study.

* * *