# Chapter 2 Data protection by design: from privacy by design to Article 25 of the GDPR

## *2.1 Introductory remarks*

This Chapter analyses the principles of privacy by design and data protection by design. The initial comparative introduction discusses the theoretical approach of regulation *by design* which has been specifically defined in the digital domain as *code is law* by Lawrence Lessig. This part briefly summarises the historical development of PbD in a comparative way by considering four significant steps of recognition in different legal frameworks.

Then, the Chapter provides an original and critical analysis of PbD by defining the advantages and disadvantages that may result from the adoption of a legal requirement for this principle. The results of this analysis have been classified in a table that compares the goals and challenges, which are further explained in detail with arguments from the legal, philosophical, economic, social, and technological domains.

The book is focused on data protection by design. Therefore, the following part of the Chapter deals with Article 25 of the GDPR by investigating and interpreting the requirement. It is important to define who shall comply with this rule, what the subject shall do, how and in which conditions. Some related provisions of the GDPR will be discussed.

Finally, the Chapter concludes by comparing PbD and DPbD concepts and by offering some notes on the need to balance the right to data protection, and DPbD, against other rights and freedoms.

## 2.2 A comparative introduction to privacy by design

The interaction between law and technology for the protection of privacy has been an object of research since the 1960s[43]. In the digital age, law and technology interact in an even closer relationship[44].

According to Lessig, in the digital world law is not the only source of rules. The four existing modalities for regulation are law, social norms, market, and architecture[45]. In the real space law regulates through consti-

---

43 *See* Alan F. Westin. *Privacy and Freedom*. Atheneum, New York, 1967. In this prominent book the author discussed the legal problems arising in the use of technological control over individuals. According to Westin, US law should have responded to the conflicts between privacy and surveillance for protecting constitutional rights.

44 The "digital age" is characterised by specific elements defined by Pascuzzi in Pascuzzi, *Il diritto dell'era digitale*, pp. 21–24. First of all, objects can be represented through bit (0 and 1). Secondly, information (a set of bits) can be processed through computers. Thirdly, information can be transferred telematically. On law and technology *see* also Vittorio Frosini. *Informatica diritto e società*. Giuffrè Editore, 1992. ISBN: 9788814039294; Natalino Irti and Emanuele Severino. "Le domande del giurista e le risposte del filosofo (un dialogo su diritto e tecnica)". In: *Contratto e impresa* 16 (2 2000), pp. 665–679; Luigi Mengoni. "Diritto e tecnica". In: *Riv. trim. dir. proc. civ.* 2 (2001), pp. 1–10; Alessandro Mantelero. "Regole tecniche e regole giuridiche: iterazioni e sinergie nella disciplina di *internet*". In: *Contratto e impresa* (2 2005), pp. 658–686; Giancarlo Francesco Ruffo et al. *Privacy digitale. Giuristi e informatici a confronto*. G. Giappichelli Editore, 2005. ISBN: 9788834858059; Giorgio Spedicato. "Law as Code? *Divertissment* sulla *lex informatica*". In: *Ciberspazio e diritto* 2 (2009), pp. 233–259; Giusella Finocchiaro. "Riflessioni su diritto e tecnica". In: *Dir. dell'informazione e dell'informatica* (4–5 2012), pp. 831–840; Francesco Romeo. "Dalla Giuritecnica di Vittorio Frosini alla *Privacy by Design*". In: *Informatica e diritto* 2 (2016), pp. 9–23.

45 *See* the first edition of the book in Lessig, *Code and other Laws of Cyberspace*.

46 *See* Lessig, *Code*, p. 5. The author explains that "we must understand how a different "code" regulates — how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is". Lessig adopted a constitutional point of view (i.e. who regulates behaviour to achieve which values). According to his perspective, cyberspace is more than the Internet and is regulated through code. Therefore, design embeds the values of whatever entity does the coding. On this matter *see* further Giovanni Sartor. "Il diritto della rete globale". In: *Ciberspazio e diritto* 4 (2003), pp. 67–94. *See* also the criticism of Lessig's approach by David G. Post. "What Larry Doesn't Get: Code, Law and Liberty in Cyberspace". In: *Stanford Law Review* 52 (2000), pp. 1439–1459; and Chris Reed. *Making laws for cyberspace*. Oxford University Press, 2012. ISBN: 9780199657605, pp. 9, 208–211. According to these scholars, Lessig took a deterministic approach to the market that did not correspond to the way it worked in that historical moment. So, the market did not have the technological

tutions, statutes, and legal codes, but in the digital space, or cyberspace, the regulation also occurs with the *code*[46]. This approach has been called *code is law*[47].

In general, law as social control creates a rule backed by sanction that shapes actors' actions[48]. Another type of law confers and defines the matter of exercise of private or public powers[49]. A legal rule can be written in a legal text that is interpreted afterwards[50]. However, this rule can also be contained in a court's decision or be implicit as *cryptotype*[51]. Generally, a legal rule is settled by a State and enforced by a court. Law regulates in defined geographical limits[52]. By contrast, technical choices of architectural regulation create an embedded set of rules. This set has been defined *lex*

---

structure that Lessig used and the interactions between the four modalities of regulation are not linear. However, they recognised that law, market, social norms and code all regulated and influenced each other.

47 "Code" denotes both software and hardware in a broad sense.

48 According to Kelsen, law is the primary norm which stipulates the sanction. *See* Hans Kelsen. *General Theory of Law and State, the 20th Century Legal Philosophy*. Oxford University Press, 1949, p. 61. *See* also for the modern age, e.g., Lee Tien. "Architectural regulation and the evolution of social norms". In: *Yale JL & Tech.* 7 (2004), pp. 1–22, p. 6.

49 Hart explained the variety of laws in Herbert Lionel Adolphus Hart. *The concept of law*. Oxford University Press, 1997, pp. 26–49. The first edition of this book dates back to 1961. Legal rules are traditionally backed by sanctions commanded by a sovereign (rules of behaviour). This is Austin's theory of law. However, Hart observed that rules conferring legislative or judicial powers are not backed by a sanction. They are recognised as rules of the system (rules of recognition). The two minimum conditions that are necessary and sufficient for validating the existence of the legal system are: 1) rules of behaviour must be obeyed by the citizens; 2) rules of recognition must be effectively accepted as common public standards (*see* this book from p. 115).

50 Francesco De Vanna. "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective". In: *Use and Misuse of New Technologies*. Springer, 2019, pp. 185–208. ISBN: 9783030056483, p. 187; Spedicato, "Law as Code? *Divertissment* sulla *lex informatica*", pp. 248–249.

51 *See* Rodolfo Sacco. "Legal formants: a dynamic approach to comparative law (installment II of II)". in: *The American Journal of Comparative Law* 39.2 (1991), pp. 343–401, p. 385. Sacco asserted that in a legal system a specific rule could exist without being perceived. It has to be discovered because it is implicit and applied unintentionally. The cryptotype is the pattern that reveals the implicit rule, and is retrieved by the interpreter/scholar. To this end, comparative studies are fundamental because only by comparing the similarities and dissimilarities of systems is it possible to find the implicit and unrevealed rule.

52 This statement refers to the territorial sovereignty.

*informatica*[53]. The information flow in the network is regulated through a technical configuration whose jurisdiction is the network itself, and where the source of rule is not the State yet, but the rule embedded by a developer or producer[54]. In the Information Society a developer has the power to configure technical standards and to make them self-executed or automated, independently of any territory[55].

From an objective point of view, law regulates *ex post*, while architecture constraints *ex ante*[56]. People feel a norm constraint before any violation, but the rule works objectively *ex post*. Therefore, from a subjective perspective, it has been claimed that the technical rule is not perceived by people as in the case of law[57]. Architectural regulation directly influences the structure of the actions, and the deterrent effect does not guide actors' behaviour yet[58]. Thus, technology engages with what is possible straightaway[59].

Code regulates phenomena in parallel with the law. They are both a source of rules. Technical regulation does not substitute the traditional regulation. Who creates the technical rule, and who the code writer is, are

---

53 *See* Joel R. Reidenberg. "Lex informatica: The formulation of information policy rules through technology". In: *Tex. L. Rev.* 76 (1997), pp. 553–593.

54 *See* Reidenberg, *op. cit.*, p. 569. The author here compares legal regulation and *lex informatica* in a comparative and interesting table. On extraterritoriality of cyberspace *see* Reed, *Making laws for cyberspace*, pp. 29–47.

55 On the regulation by software *see* the critical approach in James Grimmelmann. "Regulation by software". In: *Yale LJ* 114 (2004), pp. 1719–1758. Information Society has been defined as a complex concept by Webster in the first chapter of Frank Webster. *Theories of the information society*. Routledge, 2006. ISBN: 9780415406338. According to this scholar, any definition should take into account technological and economic aspects.

56 *See* Maja Van der Velden. "Design as regulation". In: *International Conference on Culture, Technology, and Communication*. Springer. 2016, pp. 32–54, p. 37. Here the useful example is divided into objective and subjective perspectives. The former identifies how the constraint is observed when imposed, while the latter corresponds to when it is experienced. Firstly, architecture constrains up front like a locked door and law instead operates later on, like the rule on theft. Secondly, architecture and law constrain before the act from a subjective point of view. The author further elaborated Lessig's classification of objective and subjective perspectives. *See* the other edition of the work in Lessig, *Code*.

57 Here, law means the rule established in the community that has the power to influence and control actions. *See* Tien, "Architectural regulation and the evolution of social norms", pp. 15–16.

58 Tien, *op. cit.*, p. 7.

59 *See* Roger Brownsword. "Law, liberty and technology". In: *The Oxford handbook of law, regulation and technology*. Oxford University Press, 2017, pp. 41–68, p. 55.

questions that relate to the distribution of powers. On the one hand, design power belongs to private actors (e.g. developers, companies, Internet giants, etc.), which generally produce a product or offer a service. On the other hand, law can establish binding rules applicable to these products and services and their related technologies. It thus can be argued that law can interfere with the code and can change its regulation, just as it does with the market or with the architecture of buildings.

Furthermore, technology absorbs values and goals during the development process[60]. Developers may be unconscious of this reflection of values[61]. Nonetheless, design is never neutral and could embed social values[62]. Jurists assume that these values are embedded in constitutions, charters and legal provisions. Defining principles and values is strictly related to a specific society and its context. However, a change in perspective can help highlight that wherever technology is not neutral, and it is instead related to a set of values. Therefore, as Lessig suggests in his prominent book, in the digital age mankind can architect cyberspace in order to protect values that people recognise as fundamental[63].

Technological innovation could be considered an opportunity to embed political values in artefacts[64]. Thus, engineering and law should cooperate in shaping technology and taking advantage of the respective regulatory potential[65]. The wording "regulating code to regulate better"[66] suggests that technology, and its design, if regulated by law, could be used for

60 Technical choices are never neutral. *See* De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 197. The author wrote that the assumption of neutrality is illusory.

61 *See* Laurence Diver and Burkhard Schafer. "Opening the black box: Petri nets and Privacy by Design". In: *International Review of Law, Computers & Technology* 31.1 (2017), pp. 68–90, p. 74.

62 *See* Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, pp. 23, 43–51.

63 Lessig, *Code*.

64 *See* the sociological discussion in Bryan Pfaffenberger. "Technological dramas". In: *Science, Technology, & Human Values* 17.3 (1992), pp. 282–312. According to this scholar, political values are produced in society. In this work the term political assumes a higher meaning than the one related to factions and parties.

65 *See* De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 196. The author also added ethics in the relation between law and engineering creating a pluralistic perspective, which follows Lessig's suggestion on the *code is law* approach.

66 Lessig, *Code*, p. 114.

embedding legal principles and addressing legal problems in various contexts[67].

This might be the case of privacy and data protection concerns in cyberspace[68]. Indeed, the regulatory potential of law could be exploited for the protection of privacy- and data protection-related issues.

In brief, the right to privacy was first presented in a prominent American study as the principle that protects the "inviolate personality" of an

67 The technological regulation is frequently used for protecting intellectual property rights. The problem here is the growing number of infringements of copyrights that occur in the digital age. Protecting the digital expression of the intellectual work (DVD, CD, etc.) is the aim of the development of new tools and methods. The term Digital Rights Management (DRM) identifies the technologies that generally allow copyright owners to keep under control access to and use of digital content. For example, some DRM systems protect content against copying and are installed on consumers' devices. Different legal frameworks provided anti-circumvention provisions for defending DRM, such as in the US (Digital Millennium Copyright Act (DMCA) of 1998) and in the EU (Copyright Directive of 2001). As regards DRM systems, *see* Roberto (ed.) Caso. *Digital Rights Management. Problemi teorici e prospettive applicative. Atti del convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 e 22 marzo 2007*. Quaderni del Dipartimento di Scienze Giuridiche, n. 70 dell'Università di Trento, 2008. ISBN: 9788884432193; Roberto Caso. *Digital Rights Management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*. Privacy e innovazione. Trento: Digital Reprint. <eprints.biblio.unitn.it/4375/>, 2006; Stefan Bechtold. "Digital rights management in the United States and Europe". In: *The American Journal of Comparative Law* 52.2 (2004), pp. 323–382; Pamela Samuelson. "DRM {and, or, vs.} the law". In: *Communications of the ACM* 46.4 (2003), pp. 41–45; Dan L. Burk and Julie E. Cohen. "Fair use infrastructure for rights management systems". In: *Harv. JL Tech* 15 (2001), pp. 41–83. *See* also in relation to privacy issues Julie E. Cohen. "DRM and Privacy". In: *Berkeley Tech. LJ* 18 (2003), pp. 575–617; Lee A. Bygrave. "Privacy and data protection in an international perspective". In: *Scandinavian studies in law* 56.8 (2010), pp. 165–200; and Alessandro Palmieri. "DRM e disciplina europea della protezione dei dati personali". In: *Digital Rights Management. Problemi teorici e prospettive applicative. Atti del convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 e 22 marzo 2007*. Quaderni del Dipartimento di Scienze Giuridiche, n. 70 dell'Università di Trento, 2008, pp. 197–212. ISBN: 9788884432193. DRM is an example of *code is law* in Alessandra Quarta and Guido Smorto. *Diritto privato dei mercati digitali*. Le Monnier università, 2020. ISBN: 9788800749756, pp. 62–65, which explained how intense the control is over digital contents within this phenomenon.

68 As will soon be explained, in the European Union, the right to privacy is considered a different right from data protection historically and systematically. Therefore, this work does not use the two terms as synonyms.

individual[69]. In the European literature the debate on privacy has been assigned to a civil law category ("diritti della personalità", "droits de la personalité", "derechos de la personalidad"), which groups the individual rights that are granted to a natural person for protecting intimate spheres, private life and personality in a physical dimension[70]. Since the definitions of privacy may often differ, conceptualising it is very complex and requires scholars to adopt different or pragmatic approaches[71]. For decades, legislators, authorities and courts around the globe have been creating a regulatory framework for the protection of privacy and personal data[72]. In recent

69 *See* Samuel D. Warren and Louis D. Brandeis. "Right to privacy". In: *Harv. L. Rev.* 4 (1890), pp. 193–220. On this paper *see* further Chapter 4, Section 4.2.

70 *See* Giorgio Resta. "Personnalité, Persönlichkeit, Personality: Comparative Perspectives on the Protection of Identity in Private Law". In: *European Journal of Comparative Law and Governance* 1.3 (2014), pp. 215- 243; Giorgio Resta. *Dignità, persone, mercati*. G. Giappichelli Editore, 2014. ISBN: 9788834849323, pp. 73–74. *See* also Guido Alpa and Giorgio Resta. *Le persone e la famiglia. Vol. 1: Le persone fisiche e i diritti della personalità*. Wolters Kluwer Italia s.r.l., 2019. ISBN: 9788859820871, pp. 145–163.

71 On this regard, *see* Daniel J. Solove. "Conceptualizing privacy". In: *Calif. L. Rev.* 90 (2002), pp. 1087- 1156. *See* also Dan Feldman and Eldar Haber. "Measuring and protecting privacy in the always-on era". In: *Berkeley Tech. LJ* 35 (2020), pp. 197–250.

72 The first data protection law is the Hessisches Datenschutzgesetz [1970] GVBl I 625 of the German State Hesse. For a useful synthesis of the historical development of privacy and data protection in the EU *see* Thomas Steinz. "The Evolution of European Data Law". In: *The Evolution of EU Law*. Oxford University Press, 2021. ISBN: 9780199592968; Christopher Kuner et al. *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 2–47; Hielke Hijmans et al. *The European Union as guardian of internet privacy*. Springer, 2016. ISBN: 9783319340906, pp. 39–58; Orla Lynskey. *The foundations of EU data protection law*. Oxford University Press, 2015. ISBN: 9780198718239; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamento europeo*; Ronald Leenes et al. *Data protection and privacy: the age of intelligent machines*. Hart Publishing, 2017. ISBN: 9781509919345. As regards the US framework, *see* Daniel J. Solove and Paul M. Schwartz. *Information privacy law*. Wolters Kluwer Law & Business, 2018. ISBN: 9781454892755; the recent analysis in Neil M. Richards and Woodrow Hartzog. "Privacy's Constitutional Moment". In: *SSRN: <ssrn.com/ abstract=3441502>* (2019); Madeleine Schachter. *Informational and decisional privacy*. Carolina Academic Press, 2003. Internationally, *see* Lee A. Bygrave. *Data privacy law: an international perspective*. Vol. 63. Oxford University Press, 2014. ISBN: 9780199675555. At the international level, in 1948 the right to privacy was recognised as a fundamental right in the Universal Declaration of Human Rights (Article 12). In 1950, the right to respect for private life was affirmed in the European Convention on Human Rights (Article 8). With the advent of ICTs, the Convention for the Protection of Individuals

years, the advent of the digital age has linked the right to privacy with the concepts of "data" and "information". The digital environment has challenged the protection of the right to privacy conceived by scholars as "the right to be let alone"[73]. In 1967, the prominent US scholar Westin wrote that the increased collection and processing of information could lead to a "sweeping power of surveillance by government over individual lives and organisational activity"[74]. In the EU the right to data protection developed as a separated right[75]. The wording "data protection" derives from the German "datenschutz"[76]. This nomenclature better identifies the interest in protecting personal data as information out of a spatial dimension[77]. The Charter of Fundamental Rights of the European Union adopted this separate approach by recognising the respect for private and family life and the protection of personal data separately, and respectively, by Articles 7 and 8[78].

---

with regard to Automatic Processing of Personal Data became the only legally binding international instrument in the data protection field. On this regard, *see* Christos Giakoumopoulos, G. Buttarelli, and M. O'Flamerty. *Handbook on European data protection law*. European Union Agency for Fundamental Rights and Council of Europe, Luxembourg, 2018. ISBN: 9789294919014, pp. 24–27.

73 In the foundational text *The Right to Privacy* by Warren and Brandeis the tort of privacy aimed at protecting people against media and press (so-called yellow journalism). However, as Barbas pointed out in her investigation, this tort failed to address the new concerns of ICTs. *See* in Samantha Barbas. "Saving privacy from history". In: *DePaul L. Rev.* 61 (2011), pp. 973–1048. She describes the history of the right in the US from 1890 to the Modern Era. It is worth noting that after the analysis she concludes that privacy should be defined in holistic terms, having regard to technology, social norms and media practices. Privacy is not a rigid and static right.

74 Westin, *Privacy and Freedom*, p. 158.

75 *See* Hijmans et al., *The European Union as guardian of internet privacy*, p. 17.

76 *See* Bygrave, "Privacy and data protection in an international perspective", p. 168.

77 Bygrave, *op. cit.*

78 Article 7 "Respect for private and family life" states: "Everyone has the right to respect for his or her private and family life, home and communications". Article 8 on "Protection of personal data" reads as follows: "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".

Under EU law, privacy and data protection are different fundamental rights, but they are closely connected[79]. As defined by Hijmans, the former right is a normative value, while the latter represents the legal structure that allows individuals to claim fair and lawful data processing[80]. In international contexts this distinction is not always appropriate because in some legal frameworks the term privacy could also be used for regulating the processing of personal data[81]. Regardless of any differences, both rights represent constitutional values that have to be guaranteed[82].

As mentioned in the introductory remarks, the huge collection of personal data and the multiple sources of invasions characterise the digital age. To date, several studies have investigated the relationship between

79 In Hijmans et al., *The European Union as guardian of internet privacy*, p. 62 the author explained why they are not identical concepts in the EU system. As mentioned, the Charter of Fundamental Rights of the European Union contains two different rights. In Bart Van der Sloot. "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?" In: *Data protection and privacy: (In)visibilities and infrastructures*. Springer, 2017, pp. 3–30. ISBN: 9783319507965, Van der Sloot analysed these rights and explained that with GDPR the reference to the right to privacy has been deleted in the data protection texts (in the Data Protection Directive 95/46 there were lots of references, e.g. Article 1). This choice highlights the disconnection between privacy and data protection. So, the rights are nowadays treated by the literature as independent. On the distinction *see* also Juliane Kokott and Christoph Sobotta. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR". in: *International Data Privacy Law* 3.4

80 *See* Hijmans et al., *The European Union as guardian of internet privacy*, p. 6. Data protection is more specific than privacy because it is focused on data. The same author proposed the following solution: privacy is why protection is needed, whereas data protection is how protection is delivered. Bygrave agreed with this view in Bygrave, "Privacy and data protection in an international perspective".

81 As discussed in Chapter 4, in the US system the term is also associated with the protection of information related to an individual. Informational privacy is associated with the rules governing data collection. *See* e.g. Ronald Leenes and Bert-Jaap Koops. "'Code' and privacy-or how technology is slowly eroding privacy". In: *SSRN: <ssrn.com/abstract=661141>* (2005), p. 6.

82 Under EU law, according to Article 16 of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning them. This article represents the legal basis for the adoption of rules on data protection under EU law. As mentioned, in the EU system, privacy and data protection are also protected according to Articles 7 and 8 of the Charter of Fundamental Right, which has the same legal value as the constitutional treaties of the EU. *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*.

code and privacy[83]. The interaction between law and design could address some issues. Architectural regulation could be manipulated to protect privacy and data protection as functions of design, as door-closing does[84].

In this field, the concepts of *privacy by design* and *data protection by design* have been proposed by scholars and policy makers to mitigate concerns and achieve legal compliance, by taking into account how technology is designed. Moreover, even beyond the design implementation, policies and organisational strategies are still very important for these principles. PbD and DPbD are, indeed, global approaches. As will be explained later, the difference between PbD and DPbD is not merely related to the use of "privacy" or "data protection" in their expressions. It will be necessary to differentiate and compare the concepts accurately.

The expression *privacy by design* defines the approach that proposes to build privacy principles and provisions into the design and architecture of ICTs so as to improve legal compliance[85].

In the 1990s, Cavoukian pioneered the concept of PbD by creating a framework based on proactive and preventive solutions for protecting privacy[86]. In her words, PbD is "an engineering and strategic management

---

83 *See* e.g. three prominent studies that discussed this interaction from a legal theory perspective: Lessig, *Code and other Laws of Cyberspace*; Tien, "Architectural regulation and the evolution of social norms"; Leenes and Koops, "'Code' and privacy-or how technology is slowly eroding privacy".

84 Tien, "Architectural regulation and the evolution of social norms", p. 14.

85 According to Koops and Leenes, PbD can be defined as "the principle or concept according to which privacy should be built into systems from the design stage and should be promoted as a default setting of every ICT system". *See* Bert-Jaap Koops and Ronald Leenes. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law". In: *International Review of Law, Computers & Technology* 28.2 (2014), pp. 159–171, p. 159.

86 *See* the presentation of the approach in Ann Cavoukian. "Privacy by design". In: *Information and privacy commissioner of Ontario, Canada* (2009). The PbD features should be embedded in the design specifications and implemented in the networked infrastructure and business practices. The former Privacy Commissioner of Ontario produced a number of studies on PbD from both theoretical and applied perspectives. *See* the research in Ann Cavoukian. "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D". In: *Identity in the Information Society* 3.2 (2010), pp. 247–251; Ann Cavoukian. "Operationalizing privacy by design: A guide to implementing strong privacy practices". In: *Information and privacy commissioner of Ontario, Canada* (2012); Ann Cavoukian. "Privacy by design: leadership, methods, and results". In: *European Data Protection: Coming of Age*. Springer, 2013, pp. 175–202. ISBN: 9789400751705; Ann Cavoukian. "Evolving FIPPs: proactive approaches to privacy, not privacy paternalism". In: *Reforming European Data Protection Law*. Springer, 2015, pp. 293–309.

approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls"[87].

Thus, this concept aims to achieve strong privacy protection before the invasion of the private sphere and the violation of the rule occur[88]. In an effort to share her approach, Cavoukian developed seven the Foundational Principles of Privacy by Design[89]. These are framed as follows, without hierarchy:

1. "Proactive not reactive, Preventative not remedial". The PbD approach aims to pre-empt privacy risks by identifying them in the design stage through a Privacy Impact Assessment. Technological measures should thus be combined with risk management and an organisational set-up. Privacy breaches should be prevented before they occurr. The leadership of a company has the responsibility to adopt this principle in its management by executing a privacy programme;
2. "Privacy as the Default Setting". The default rule means that data systems and business practices shall automatically protect data. The data subject has the option to do nothing and still be protected by default. To this end, minimising the collection of information is central;
3. "Privacy Embedded into design". Within PbD it is fundamental to embed privacy into the design as a component of the system without diminishing its functionality. Research by Cavoukian and the IPC's office shows that the incorporation is achievable;
4. "Full functionality – Positive-sum, Not zero-sum". The PbD approach aims to accommodate all stakeholders' interests in a win-win deal. Business interests are legitimate and should coexist with privacy. The

---

ISBN: 9789401793858. All the papers and books are collected at <www.ryerson.ca >. Last accessed 06/10/2021.

87 Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices", p. 8.

88 Cavoukian often remarked that *privacy by Design comes before-the-fact, not after*. *See* e.g., Cavoukian, "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D", p. 249.

89 *See ex multis* Ann Cavoukian. "Understanding How to Implement Privacy by Design, One Step at a Time". In: *IEEE Consumer Electronics Magazine* 9.2 (2020), pp. 78–82; Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices", pp. 3–4; Ann Cavoukian et al. "Privacy by design: The 7 foundational principles". In: *Information and privacy commissioner of Ontario, Canada 5* (2009), p. 1. On these principles *see* also the Guide by the Spanish DPA: AEPD Agencia Espanõla de Protección de Dados. *A Guide to Privacy by Design*. AEPD, 2019, pp. 7–10.

"privacy vs. security" dichotomy may be replaced by "privacy and security" because it is possible to maintain both;

5. "End-to-end security – full lifecycle protection". PbD is applied to the entire data life- cycle even before the collection of information and up to the erasure or the destruction of the assets where it is stored;
6. "Visibility and transparency – keep it Open". The data subject must be aware of the collection and of its purpose. The processing operations and business practices should be transparent and clear for the individual;
7. "Respect for User Privacy – keep it User-Centric". Within PbD, the data subject's interests shall be central even if they are not explicitly expressed. So, high importance should be given to privacy-friendly settings and privacy notices[90].

According to Cavoukian, PbD principles are adaptable and relevant for any of the PbD application areas[91]. The PbD framework has both an internal level (e.g. the design of ICTs) and an external one (the organisational steps of the business practices). For addressing privacy concerns, particular importance was attributed to security by default[92].

---

90 The term "notice" is usually used in common law systems, such as the Canadian framework. Under EU law, the information provided to the data subject is collected in the "privacy policy" in accordance with Articles 12, 13 and 14 of the GDPR. *See infra* Section 2.4.8.

91 In Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices", p. 6, the areas are listed as: 1) CCTV/Surveillance Cameras in Mass Transit Systems; 2) Biometrics Used in Casinos and Gaming Facilities; 3) Smart Meters and the Smart Grid; 4) Mobile Devices and Communications; 5) Near Field Communications (NFC); 6) RFIDs and Sensor Technologies; 7) Redesigning IP Geolocation Data; 8) Remote Home Health Care; 9) Big Data and Data Analytics. Studies have been carried out in these contexts thanks to a fruitful collaboration with private stakeholders. *See* e.g Ann Cavoukian and Marilyn Prosch. *The roadmap for privacy by design in mobile communications: A practical tool for developers, service providers, and users*. Information and Privacy Commissioner of Ontario, 2011 and Ann Cavoukian et al. "Biometric encryption: creating a privacy-preserving 'Watch-List' facial recognition system". In: *Security and privacy in biometrics*. Springer, 2013, pp. 215–238. ISBN: 9781447152309; Cavoukian, "Understanding How to Implement Privacy by Design, One Step at a Time".

92 *See* Ann Cavoukian. *Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head*. 2017. The discussion here is focused on the public security issue. It is commonly perceived that more information is collected, more public safety and security are in place. However, this paradigm sacrifices a balance between privacy and security and the positive sum between them obtained

The framework is overtly based on the Principles of Fair Information Practices (hereinafter: FIPs)[93]. In 1973, the US Department of Health, Education & Welfare first defined the FIPs in the Report *Code of Fair Information Practice* with the aim of establishing safeguard requirements with a legal effect against automated personal data systems[94]. The authority distinguished the principles for two types of technologies – i.e. administrative automated personal data systems and systems used exclusively for statistical reporting and research – as minimum standards practices for protecting individuals[95]. Any violation would have been subject to sanctions[96].

FIPs were extended internationally in the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980[97]. These Guidelines were revised in 2013 to create the OECD Privacy Framework[98]. The OECD's basic principles are listed as follows: "collection limitation principle, data quality principle, purpose specification principle,

---

with PbD approaches. According to Cavoukian, fostering technologies to this end is fundamental (and possible) even for policies against terrorism.

93 In Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices",
p. 8, Cavoukian stressed that FIPs' perspectives inform her PbD principles (and, above all, the purpose specification and use limitation principles).

94 *See* Education & Welfare US Department of Health. *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records Computers and the Rights of citizens*. United States, DHEW Publication NO. (OS)73–94. 1973. *See* at <www.justice.gov/opcl/docs/rec-com-rights.pdf>. Last accessed 06/10/2021.

95 *See* US Department of Health, *op. cit.*, p. 41. The five basic principles were defined as follows: 1) "There must be no personal-data record-keeping systems whose very existence is secret; 2) There must be a way for an individual to find out what information about him is in a record and how it is used; 3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; 4) There must be a way for an individual to correct or amend a record of identifiable information about him; 5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data". Moreover, it was specified that deviations from the principles were allowed only exceptionally (*see* from p. 42).

96 The authority stressed that a violation would constitute an unfair practice backed by civil and criminal penalties.

97 OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, in the form of a Recommendation by the Council of the OECD*. 1980. On the FIPs *see* further Chapter 4, Section 4.2.

98 *See* OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the OECD Privacy Framework*. 2013. *See* at <www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Last accessed 06/10/2021.

use limitation principle, security safeguards principle, openness principle, individual participation principle, and accountability principle"[99]. These principles affirm the individual's right to self-determination[100].

Furthermore, the global foundational influence of the OECD's principles has been recognised by legal scholars[101]. It has been noted that these principles are highly influential internationally and serve as a bedrock foundation for privacy regulation policies[102]. It can thus be suggested that Cavoukian's principles are evidently based on the FIPs, especially as regards the visibility, transparency and user-friendly principles (PbD principles 5, 6, and 7).

Cavoukian's research as Ontario's Privacy Commissioner was quite successful internationally. Four notable examples and steps can be given before the introduction of a critical analysis on the concept of PbD.

Firstly, in 2009 the Article 29 Data Protection Working Party and Working Party on Police and Justice advocated for incorporating the principle of PbD into a new data protection framework of the EU[103]. According

---

99 *See* Part Two "Basic Principles of national application in the OECD's Privacy Framework". In this new version of the principles there are references to PbD as an innovative initiative. *See* the Report at the supplementary explanatory memorandum, pp. 103–105. Firstly, PbD is presented in connection with the Privacy Impact Assessment. Secondly, PbD could be an expression of the privacy management programme and the accountability principle, which is established in Part Three "Implementing Accountability" of the Guidelines.

100 Deirdre K. Mulligan and Jennifer King. "Bridging the gap between privacy and design". In: *U. Pa. J. Const. L.* 14 (2011), pp. 989–1034, p. 999.

101 *See* e.g. Marc Rotenberg. "Fair information practices and the architecture of privacy (What Larry doesn't get)". In: *Stan. Tech. L. Rev.* (2001), pp. 1–35, p. 16; Solove, "Conceptualizing privacy", p. 592; Mulligan and King, "Bridging the gap between privacy and design", p. 991; Ira S. Rubinstein and Nathaniel Good. "Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents'". In: *Berkeley Technology Law Journal* 28 (2013), pp. 1333–1409, p. 1344; Neil Richards and Woodrow Hartzog. "Taking trust seriously in privacy law". In: *Stan. Tech. L. Rev.* 19 (2015), pp. 431–472, p. 458.

102 *See* Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, p. 59.

103 *See* WP29 Article 29 Working Party, Working Party on Police, and Justice. *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*. 02356/09/EN, WP 168, 2009. The former Working Party (WP29) was institutionalised by article 29 of Directive 95/46 and had an advisory status acting independently from the other EU institutions. In accordance with Article 29, the WP was composed of one "representative of the supervisory authority or authorities designated by each Member State and of a representative of the

to the authorities, PbD represented a tool for innovating the framework and protecting against technological developments. ICTs should integrate privacy and data protection in their design settings by default. To this goal, a broad and consistent legal principle should be introduced in the law[104]. The requirement should be binding for data controllers, technology designers and producers at an early planning stage of ICTs, whose development should avoid or minimise the amount of personal data processed. Privacy-enhancing technologies (hereinafter: PETs) should be used in order to enhance security[105]. The principle of PbD should be framed in a flexible and technologically neutral way in order to be applied on a case-by-case basis and to be consistent regardless of time and context[106]. As will be explained in detail, the proposal of the GDPR and its final text contain a PbD requirement that assume some of the mentioned characteristics.

Secondly, with the Resolution on Privacy by design the concept gained global approval[107]. The 32nd International Conference of Data Protection Authorities and Privacy Commissioners emphasised PbD as a holistic concept and essential component of fundamental privacy protection. The Resolution recognised that a more robust approach is necessary for addressing the challenges to privacy and fully protecting individuals from the effects of the information life cycle in the ICTs. According to the Resolution, PbD principles should be promoted in the regulatory frameworks and beyond policies and rules (e.g. at organisational and research levels). Actually, the text listed Cavoukian's principles to encourage their legal adoption in countries[108]. Therefore, the Commissioners agreed that privacy should be embedded into design as a default protection. This Resolution was not legally binding. However, it can be argued that after its landmark adoption

---

authority or authorities established for the Community institutions and bodies, and of a representative of the Commission". The authority released several guidelines on data protection law contributing to the uniform application of the norms. It ceased to exist on 25 May 2018 and European Data Protection Board (EDPB) replaced it.

104 *See* Article 29 Working Party, Police, and Justice, *op. cit.*, p. 13.

105 For the notion of PETs *see infra* Section 2.3.

106 *See* Article 29 Working Party, Police, and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, p. 14.

107 32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, Jerusalem, Israel (27–29 Oct 2010).

108 It is worthy of note that the Former Commissioner personally encouraged the adoption of the PbD principles during the conference.

PbD was added to the agendas on data protection thanks to the promotion of data protection Authorities within their respective jurisdictions[109].

Thirdly, in 2011 in the US legal framework a Commercial Privacy Bill of Rights was proposed to protect consumer privacy[110]. This bill has set a provision concerning PbD, but it was never approved by Congress[111]. Under the proposed Section 103, the privacy by design requirement would have obligated a covered entity to implement a comprehensive information privacy programme proportionally to the size, type, and nature of the information collected. This programme should have been implemented by two categories of activities:

1. the incorporation of the "necessary development processes and practices throughout the product life cycle" for safeguarding personally identifiable information (PII)[112]. This information is based on "the reasonable expectations" of individuals on privacy and "the relevant threats that need to be guarded against in meeting those expectations";
2. the maintenance of "appropriate management processes and practices throughout the data life cycle" for complying with provisions, privacy policies and the privacy preferences of individuals.

The elements of these provisions that are consistent with Cavoukian's version of PbD are, on the one hand, the incorporation of practices throughout the product life-cycle and, on the other hand, the attention to a compliant organisational management. Both elements were based on the individual privacy preferences and expectations. This so-called relative approach is typical in US legislation[113]. As regards the differences, the provision was limited to covered entity and it aimed to protect only consumer privacy. A covered identity was defined as the person who processes information related to more than 5,000 individuals consecutively in a year or other specified subjects in Section 401 of the Bill. Therefore, the provision would have been applied only to medium-to-large commercial companies. According to Krebs, this Bill did not fulfil the PbD idea completely, but it

109 The same intuition has been expressed in Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 164.

110 *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress (2011). The legislation was proposed by Senators John Kerry and John McCain.

111 The PbD provision was in the first Title "Right to security and accountability".

112 On the differences between PII and personal information *see*, e.g., Paul M. Schwartz and Daniel J. Solove. "Reconciling personal information in the United States and European Union". In: *Calif. L. Rev.* 102 (2014), pp. 877–916.

113 *See* Chapter 4, Section 4.2.

gave signals of its importance[114]. However, as mentioned, the text was only introduced in the Senate without any successful approval. Even Canadian scholars analysed the proposal, but despite the great contribution to the debate, a PbD requirement was never included in Canadian legislation, either[115].

Fourthly, PbD has been included by the Federal Trade Commission (FTC or the Commission) as a recommended business practice to promote the protection of consumer data in the US. In 2012, the FTC released the final Report "Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker" encouraging a framework of best practises for consumer privacy[116]. The Commission noted that the Report aims to boost best practices without conflicting with other applicable statutory requirements[117]. The FTC called on Congress to extend privacy and security legislation and on companies to self-regulate their practices according to the recommendations. The FTC's framework applies to information that can be reasonably linked to a specific consumer, computer, or another device because it can identify an individual[118]. The companies that collect or use personally identifiable information are subject to the recommendations unless they only process non-sensitive data from fewer than 5,000 consumers per year and do not share data with third parties[119].

The FTC's best practices include privacy by design, simplified consumer choice for giving more control to consumer, and increased transparency. According to the Report, PbD is recommended for commercial practices in order to incorporate substantive privacy protection at every stage of the development of products and services[120]. PbD should be implemented

114 David Krebs. "Privacy by design: Nice-to-have or a necessary principle of data protection law". In: *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 4 (2013), pp. 2–20, p. 10.

115 Krebs, *op. cit.*

116 FTC Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker*. FTC Report, 2012. The first report was issued in 2010; at the time, it received hundreds of public comments (also by European actors, such as the French DPA *Commission Nationale de l'Informatique et des Libertés*).

117 *See* Federal Trade Commission, *op. cit.*, p. 16.

118 *See* Federal Trade Commission, *op. cit.*, pp. 18–22.

119 *See* Federal Trade Commission, *op. cit.*, p. 22.

120 The baseline principle states that companies should promote consumer privacy throughout their organisations and at every stage of the development of their products and services.

systematically through substantive protections, such as data security, reasonable collection limits, sound retention practices and data accuracy[121]. While replying to the comments received in the report, the FTC explained that its framework embodies the OECD's Privacy Guidelines[122]. Moreover, the authority highlighted the importance of procedural protections for implementing the PbD principle: comprehensive data management should be maintained throughout the life-cycle of companies' products and services[123]. Thus, the FTC approach is focused on organisational measures leaving behind a more technical implementation. Nevertheless, the framework mentions PbD providing a basis for its adoption in the US[124]. In addition to the procedural program, the Commission advocated the use of privacy-enhancing technologies[125].

In sum, according to the FTC, PbD is a commercial best practice for every stage of product and service development established to protect consumer data. It can be argued that this notion is not a legally binding rule. However, it can be considered a softer kind of rule, that could be enforceable under Section 5 of the FTC Act[126]. Indeed, the FTC has a

121 *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker*, p. 23. These four examples have been defined the FTC PbD principles by Stuart L. Pardau and Blake Edwards. "The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity". In: *J. Bus. & Tech. L.* 12 (2016), pp. 227–276, p. 231.

122 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker*, p. 23.

123 *Ibid.*

124 Krebs, "Privacy by design: Nice-to-have or a necessary principle of data protection law", p. 11.

125 On the notion of privacy enhancing technologies *see* next Section 2.3.

126 Section 5 of the Federal Trade Commission Act (FTC Act), 15 USC. § 45. *See* <www.ftc.gov/ enforcement/statutes/federal-trade-commission-act>. Last accessed 06/10/2021. The FTC jurisdiction protects consumers against unfair and deceptive acts or practices by companies. This is a typical antitrust protection. However, in the same Section, the FTC expands the jurisdiction to protect consumer privacy issues. *See* Daniel J. Solove and Woodrow Hartzog. "The FTC and the new common law of privacy". In: *Colum. L. Rev.* 114 (2014), pp. 583–676, p. 598. In some instances, the authority requires adopting a comprehensive privacy programme with security measures. On the FTC's unfairness doctrine *see*, e.g. Pardau and Edwards, "The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity". According to Solove and Hartzog, the FTC's Reports help to understand its interpretation of Section 5. They are soft laws that may be enforced in the future. Under Section 5 the FTC has also the power to enforce the agreements between the EU and the US on data protection, e.g. the EU-US Privacy Shield Framework before the

prominent role of control on business practices towards US companies. According to Solove and Hartzog, the FTC jurisprudence is the most influential regulating force on privacy in the US because the statutory law is discordant, and the common law lacks rules[127]. In the US, the FTC is the closest body to a national data protection authority (hereinafter: DPA)[128].

After more than 20 years of efforts to develop and promote the concept, it finally obtained legal status in the EU where PbD has been articulated in Article 23 of the draft GDPR[129]. This Article has primarily established the obligation arising from the principle of data protection by design (and by default). The mentioned Article has been amended significantly, as will be explained in Section 2.4. Hence, the European Commission coined the wording *Data Protection by Design*.

According to the existing EU regulatory framework on data protection law, DPbD is a mandatory principle. Central is Article 25 of the GDPR. Before proceeding to examine this article, the following section will provide a critical analysis of the concept of privacy by design in order to deeply investigate the implications of the adoption and endorsement from legal, philosophical, technical, economic and societal points of view.

## 2.3 A critical analysis of privacy by design

According to Pagallo, without expecting that the technical tricks of design will ever tell us what the future of privacy will be, we can imagine that it is from design that we will be able to understand a lot about the privacy of the future[130].

---

Judgement of the European Court of Justice (Grand Chamber) of 16 July 2020 – Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, C-311/18.

127 Solove and Hartzog, "The FTC and the new common law of privacy", p. 587.

128 Demetrius Klitou. *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*. Vol. 25. Information Technology and Law Series. Springer, 2014. ISBN: 9789462650251, p. 41.

129 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/2012/011 final – 2012/0011 (COD).

130 Own English translation of the words in Ugo Pagallo. "Privacy e design". In: *Informatica e diritto* 18.1 (2009), pp. 123–134.

Prior studies have noted the importance of values in design[131]. According to Friedman *et al.*, Value Sensitive Design (hereinafter: VSD) is a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process"[132]. Thus, VSD aims to influence early on the design of technology in a proactive way[133]. In that study, privacy was considered a human value. Other scholars investigated the possibility of designing for the value of privacy[134]. By embedding values, VSD creates a so-called "normative technology"[135].

Essentially, PbD can be considered both a *code is law* and a VSD approach because it aims to design with the principles of privacy and the corresponding rules in mind[136]. PbD even goes beyond VSD because it is based on law[137].

In the privacy field, Privacy Enhancing Technologies (PETs) were invented in the 1990s to customise some information flow rules through technical design[138]. PETs identify technological mechanisms that intentionally aim to protect privacy[139]. In 1995 the first work that introduced PETs as a regulatory strategy was presented by the Information and Privacy

131 *See* e.g. Mulligan and King, "Bridging the gap between privacy and design", p. 1019; Jeroen Van den Hoven, Pieter E Vermaas, and Ibo Van de Poel. *Handbook of ethics, values, and technological design: Sources, theory, values and application domains*. Springer, 2015. ISBN: 9789400769700.

132 Batya Friedman, Peter H. Kahn, and Alan Borning. "Value sensitive design and information systems". In: *The handbook of information and computer ethics* (2008), pp. 69–101, p. 70.

133 *See* Friedman, Kahn, and Borning, *op. cit.*, p. 85. On VDS *see* also Janet Davis and Lisa P. Nathan. "Value sensitive design: Applications, adaptations, and critiques". In: *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*. Springer, 2015, pp. 11–40. ISBN: 9789400769700.

134 *See* Martijn Warnier, Francien Dechesne, and Frances Brazier. "Design for the Value of Privacy". In: *Handbook of ethics, values, and technological design: Sources, theory, values and application domains*.
Springer, 2015, pp. 432–445. ISBN: 9789400769700.

135 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 261.

136 *See* Klitou, *op. cit.*, p. 262.

137 Klitou, *op. cit.*, p. 263.

138 *See* Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 574.

139 *See* Lee A Bygrave. "Hardwiring privacy". In: *The Oxford Handbook of the Law and Regulation of Technology*. Ed. by Eloise Scotford and Karen Yeung. Oxford: Oxford University Press, 2017. Chap. 31, pp. 754–775. ISBN: 9780199680832, p.

Commissioner of Ontario and by the Dutch Data Protection Authority (the "Registratiekamer" or RGK). In their Joint Report the term "privacy technologies" refers to a variety of technologies that safeguard personal privacy by minimising or eliminating the collection of identifiable data[140]. PETs were often developed for the preservation of the values of confidentiality and anonymity. In 1997, Reidenberg described the classical PETs as technologies for securing the transmission of messages, transactions and Internet searches[141]. Then, these technologies started to achieve multiple functions, such as transparency and control. The broadening of focus reflected the expanding attention on systems' design[142]. Therefore, a prominent definition of PETs was summed up by Rubinstein as follows: these technologies are "applications or tools with discrete goals that address a single dimension of privacy, such as anonymity, confidentiality, or control over personal information"[143]. PETs can be classified according to their purposes[144]. Subject-oriented PETs limit the ability to recognise a specific subject (e.g. anonymiser), whereas other PETs are object-oriented since they protect data from identification. Transaction-oriented PETs protect the data used in a transaction (e.g. by deleting automatically) and system-oriented PETs create protected areas where the subject cannot be recognised, the object is not associated to anyone and the transaction data are deleted (e.g. secure socket layer, private communication technology or secure electronic transaction).

In a critical study on PbD, Koops and Leenes highlighted that in the last decades PETs have gained great support from policymakers and re-

---

756. In this study the author uses the term "hardwiring" to indicate the efforts of building privacy into information systems' architecture.

140 *See* H. Van Rossum, H. Gardeniers, et al. *Privacy-enhancing technologies: The path to anonymity*. Registratiekamer, Information, and Privacy Commissioner of Ontario, 1995.

141 According to the author, these are also examples of *lex informatica*. *See* Reidenberg, "Lex informatica: The formulation of information policy rules through technology", pp. 574–575.

142 *See* Bygrave, "Hardwiring privacy", p. 757.

143 *See* Ira S. Rubinstein. "Regulating privacy by design". In: *Berkeley Tech. LJ* 26 (2011), pp. 1409–1456, p. 1411. The author distinguished each category of PETs according to its purposes (e.g. preventing tracking and profiling, user control, etc.). On this topic *see* also the prominent work by Giuseppe D'Acquisto et al. *Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics*. European Union Agency for Network and Information Security, 2015, pp. 27–29.

144 *See* Pascuzzi, *Il diritto dell'era digitale*, p. 97.

searchers[145]. In 2007, the European Commission promoted the use and development of PETs to ensure that breaches of data protection rules and violations of individual's rights would be technically more difficult[146]. According to the authority, these technologies could boost a design of ICTs that minimises the processing of personal data and facilitates compliance with the law[147]. Technology has been recognised as a complementary tool to the existing legal framework and enforcement mechanisms[148]. As mentioned, in 2009 WP29 agreed on these aspects by promoting PETs along with PbD.

However, PETs are mere tools, mechanisms and instruments. By contrast, PbD is conceived as a comprehensive approach to fulfilling data protection rules. It should be pointed out that the idea of PbD first emerged with the concept of PETs, as a solution for the implementation of privacy principles[149]. Indeed, the concept of PbD is strictly related to the concept of PETs[150]. Operationally PbD could include PETs, but they are often not

145 Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", p. 159.

146 *See* EC European Commission. *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*. European Commission. COM(2007) 228 final, 2007, p. 3. The definition of PETs adopted by the Commission (borrowed from the PISA project) is: "PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system". The Commission also described some examples of PETs: automatic anonymisation of data, encryption tools, cookie-cutters, the Platform for Privacy Preferences (P3P). In sum, the authority defined three objectives: 1) supporting the development of PETs by identifying their need and technological requirements and by sponsoring concrete projects; 2) supporting the use of available PETs by data controllers, through the promotion in the ICT industry and in the public sphere, and the creation of standards and a coordination of technical rules at the national level; 3) encouraging consumers to use PETs by raising awareness and facilitating informed choices.

147 *Ibid.*, p. 3.

148 *Ibid.*, p. 4. *See* also the first part of Section 2.2.

149 Pagona Tsormpatzoudi, Bettina Berendt, and Fanny Coudert. "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity". In: *Privacy Technologies and Policy, Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7–8, 2015*. Lecture Notes in Computer Science. Springer, 2015, pp. 199–212, p. 200.

150 *See* e.g. Peter Hustinx. "Privacy by design: delivering the promises". In: *Identity in the Information Society* 3.2 (2010), pp. 253–255, p. 253; Inga Kroener and David Wright. "A strategy for operationalizing privacy by design". In: *The In-*

privacy-compliant *per se*. So, a PET can be considered a building block of PbD[151].

As mentioned, PbD shapes technologies at the service of the law[152]. Actually, PbD is an evolving framework that seeks to take privacy into account at many levels: not only the "forefront engineering life-cycle" but also "all levels of an organisation"[153]. At its core, PbD is a multifaceted concept[154].

From a legal perspective, PbD is defined broadly as regulation by design for building privacy into the design and architecture of technologies, systems and processes. Technologically, PbD is a list of measures and tools developed and implemented in a design process. Moreover, PbD involves various organisational components. Hence, it is conceivable that systems, devices and services could become "privacy-aware" and "privacy-friendly"[155]. Technology becomes more than a means; it is both a threat and a solution[156].

As noted by Bygrave, the multidimensional nature of PbD may detract from its utility[157]. The starting point for understanding PbD is the research by Cavoukian. As argued by Schartum, Cavoukian's principles are impor-

---

*formation Society* 30.5 (2014), pp. 355–365, p. 361; Simone Calzolaio. "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679". In: *Federalismi.it* 24 (2017), pp. 1–21.

151 *See* Bygrave, "Hardwiring privacy", p. 759.

152 In Tsormpatzoudi, Berendt, and Coudert, "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity", p. 201 the authors observe that from a legal perspective PbD as an approach seeks technical solutions to address legal requirements.

153 Eric Everson. "Privacy by design: Taking ctrl of big data". In: *Clev. St. L. Rev.* 65 (2016), pp. 27–43, p. 28.

154 *See* for the expression: George Danezis et al. *Privacy and Data Protection by design – from policy to engineering*. European Union Agency for Network and Information Security, 2014, p. 3; D'Acquisto et al., *Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics*, p. 21; Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 164.

155 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 262; and Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 165.

156 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 294.

157 Bygrave, "Hardwiring privacy", p. 758.

tant elements, but they are formulated as slogans[158]. So, despite the potential, the principle is not immune to criticism[159].

In order to provide a detailed investigation into the concept, the following theoretical and critical analysis allows a deeper insight into the idea of PbD by comparing and discussing the edges and disadvantages that could emerge with such a legal requirement.

The elements are classified in the following Table 2.1[160]. The first column list shows the advantages, and the second the respective disadvantages. The statements have been elaborated through a legal analysis, further based on remarks and arguments made by prominent scholars in the literature. This comparison attempts to show the effects of PbD on theories of law, rights and duties, on democracy, on the digital economy, and on technology and innovation.

The table is followed by a critical analysis of the lines. The order of discussion follows the horizontal line of the table. Every advantage is briefly elucidated just before the respective disadvantage with arguments from different disciplines. As regards the legal aspects, the investigation is not limited to a particular legal framework. If necessary, the discussion will specify the legal systems from time to time. The legal analysis assumes a primary role, but arguments from philosophy, economic theory, and social and technology studies are also presented. Moreover, the arguments are not related to the concept of PbD solely. Criticism and benefits of the *code is law* or of the *regulation by technology* approaches are discussed. Since some arguments raise complex and general debates at the theoretical level (e.g. on interpretation of the law), the examination of which are outside

158 *See* Dag Wiese Schartum. "Making privacy by design operative". In: *International Journal of Law and Information Technology* 24.2 (2016), pp. 151–175, p. 157. On the same opinion, *see* Rubinstein and Good, "Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents'", p. 1338. They wrote that the seven foundational principles are not of great assistance in applying the FIPs. These principles are more inspirational than practical.

159 Actually, according to Gürses *et al.* from the principles it is not clear what the term "privacy by design" means. *See* Seda Gürses, Carmela Troncoso, and Claudia Diaz. "Engineering privacy by design". In: *Computers, Privacy & Data Protection. International Conference on Privacy and Data Protection* 14.3 (2011), pp. 1–25, p. 3.

160 The table was first presented in Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 166. However, the discussion on the elements was not included in said work. Moreover, the content of the lines has been partly reformulated and ordered in a different and more coherent way in order to provide a more detailed and incisive explanation.

the scope of the present work, the analysis will limit the discussion to the connection with PbD, in order to highlight advantages and challenges of its endorsement and implementation.

*Table 2.1 Classification of the advantages and challenges of PbD*

| ADVANTAGES AND GOALS | DISADVANTAGES AND CHALLENGES |
|---|---|
| 1. PbD legal requirement is flexible and applicable to various contexts | A broad definition means difficult implementation |
| 2. PbD legal requirement is technologically neutral | Specific solutions must be provided for each technical context |
| 3. PbD improves the effectiveness of the law and empowers the rights of the data subject | Translating principles, values and rights into machine-readable language is a challenge |
| 4. PbD aims to implement rules, principles and values | Legal interpretation is flexible and dynamic. It is hard to define common principles in different legal frameworks. Conflicts between values are possible in the design stage |
| 5. PbD promotes proactive and preventive measures | The State delegates privacy regulation to companies. Private self-regulation may be incompatible with the democratic procedures of law making and law enforcement |
| 6. PbD prevents privacy breaches before they happen | Every embedded technical solution is rigid. Therefore, it is necessary to update measures frequently |
| 7. PbD is a global approach | Building privacy is critical for developers and not possible in every situation. Not all the provisions of data protection can be automated |
| 8. PbD requires concrete organisational measures | Companies sometimes lack knowledgeable organisation |
| 9. PbD requires effective measures and less bureaucratic solutions | PbD implementation demands investments and allocated resources |
| 10. PbD can increase privacy culture in society | There is a difficulty of comprehension of the topic for the layperson |

| ADVANTAGES AND GOALS | DISADVANTAGES AND CHALLENGES |
|---|---|
| 11. PbD can increase trust and confidence in products and services | In society there is an information asymmetry and a widespread lack of knowledge on design strategies |
| 12. PbD increases consumer satisfaction and could be an opportunity for business | Collecting and commercialising personal data are the core business of many companies |
| 13. There is a business opportunity for certifications and standards | Certification does not automatically mean compliance with the law |
| 14. PbD fosters the design of new privacy friendly technologies | Adapting the existing technologies is not easy |
| 15. There will be control over and ethics of the technology | There will be barriers to innovations |
| 16. PbD aims to implement user-centric technologies | There might be increasing costs for access to digital technologies |

Firstly, PbD can be included in a legal provision, and many privacy scholars have advocated for its explicit introduction in legislation[161]. According to Krebs, PbD as an organisational best practice is not sufficient, and has to be at the core of a legislative framework on privacy and data protection[162]. To this end, the provision on PbD shall be well drafted, clearly worded, and should avoid unnecessary ambiguity.

161 *See* e.g. Hustinx, "Privacy by design: delivering the promises"; Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices"; Gürses, Troncoso, and Diaz, "Engineering privacy by design"; Mireille Hildebrandt. "Legal protection by design: objections and refutations". In: *Legisprudence* 5.2 (2011), pp. 223–248; Rubinstein, "Regulating privacy by design"; Krebs, "Privacy by design: Nice-to- have or a necessary principle of data protection law"; Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*; Tsormpatzoudi, Berendt, and Coudert, "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity"; Wiese Schartum, "Making privacy by design operative"; Giorgia Bincoletto. *La privacy by design. Un'analisi comparata nell'era digitale*. Privacy e innovazione. Roma: Aracne editrice, 2019. ISBN: 9788825524000.

162 Krebs insisted for Canadian systems particularly. *See* Krebs, "Privacy by design: Nice-to-have or a necessary principle of data protection law", p. 15.

So, such a legal requirement should mandate the approach and it could define some criteria for the design process[163]. If PbD is legally prescribed, liability and enforcement mechanisms should be in place[164]. Subjects should be accountable and liable[165]. It is worth noting that a legal provision should be established either for developers, who are the subjects that concretely arrange the design, or for data controllers[166]. The definition of data controller is not uniform in the legal frameworks. For the purpose of this section, data controller means "a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf"[167]. Public institutions, organisations and agencies, and private companies should all embrace PbD.

Moreover, PbD requirements should be comprehensive, flexible and defined in a technologically neutral way in order to be applicable over time and in different contexts[168].

---

163 Bygrave, "Hardwiring privacy", p. 767, which also refers to standards.

164 As far as the present work is concerned, Privacy by design has been indirectly employed in some case law of the FTC and the Canadian Privacy Commissioner. As regards the cases, *see* Bincoletto, *La privacy by design. Un'analisi comparata nell'era digitale*, pp. 101–132. The most interesting cases in the US are *FTC v. FrostWire* and *FTC v. Google* of 2011, and *FTC v. Wyndham* of 2014. In Canada they are *Office of the Privacy Commissioner of Canada v. Google* of 2011 and *Office of the Privacy Commissioner of Canada v. WhatsApp* of 2012.

165 It may even be argued that subjects could be sanctioned for defective design of products and services. *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 308. The scholar specified that liability should be subject to exemptions in the case of unlawful use or modification of the product/service and in the case of unlawful implementation by using a "state of the art" criterion of interpretation.

166 Klitou, *op. cit.*, pp. 268, 295. According to Klitou, directing requirements to data controllers only overesti- mates their capabilities and resources. Moreover, in a ubiquitous information society, where often there are cross-border data flows, the identity of the controllers is not easily determined. On the subjects of the law *see infra* Section 2.4.1.

167 This is the OECD's definition. *See* OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the OECD Privacy Framework*, p. 13.

168 *See* Article 29 Working Party, Police, and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, p. 14. On technical neutrality *see infra*. *See* also EDPS European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*. 2010, p. 8.

The principle should be applied on a case-by-case basis for it to be very concrete[169]. In fact, a rigid approach to PbD would be counter-productive because solutions cannot be "one-size-fits-all"[170]. They are normally tailored to a particular system or service (i.e. on an *ad-hoc basis*).

As regards the broad applicability, from a theoretical point of view jurisdiction does not seem critical for *lex informatica* because it may be applied on a transnational basis[171]. In this sense, *regulation by design* seems more flexible than *regulation by law* because it may be distributed at a global level. After the Resolution on Privacy by design, the concept is recognised as a transnational principle[172]. It has been argued that extra-territorial legal

169 *Ibid.*

170 Avner Levin. "Privacy by Design by Regulation: The Case Study of Ontario". In: *Can. J. Comp. & Contemp. L.* 4 (2018), pp. 115–159, p. 155.

171 Reidenberg, "Lex informatica: The formulation of information policy rules through technology", pp. 577- 578.

172 A summary of the legal history in three legal frameworks (US, Canada and EU) is provided here. On PbD history *see* also Calzolaio, "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679". As previously mentioned, in the US the proposal in the Commercial Privacy Bill of Rights tried to include PbD in the US framework at the federal level. However, the Bill did not obtain the (hoped-for) approval of Congress, so the US framework does not have laws that explicitly and expressly includes PbD. US law on privacy is not uniform since there are both federal and national privacy-focused regulations. *See* e.g. Privacy Act of 1974, Children's Online Privacy Act of 1998, California Consumer Privacy Act of 2018. The US scholars recognised that in the context of law and technology this sector-based regulation is less efficient than a global and general approach to privacy. *See* e.g. Helen Nissenbaum. "From preemption to circumvention: if technology regulates, why do we need regulation (and vice versa)". In: *Berkeley Tech. LJ* 26 (2011), pp. 1367–1386. On US privacy *see* further Chapter 4. In spite of the work of the Privacy Commissioner in the 1900s, the Canadian legal system does not provide a legal requirement on PbD. The Canadian framework is divided into ten provinces where privacy is regulated at the federal level by the Personal Information Protection and Electronic Documents Act (SC 2000, c 5 "PIPEDA"). Some case studies in Ontario showed that PbD in Canada had limited engineering use, but great organisational potential. *See* the presentation and discussion on the studies in Levin, "Privacy by Design by Regulation: The Case Study of Ontario". On the Canadian law for privacy and data protection *see* Federica Giovanella. *Copyright and Information Privacy: Conflicting Rights in Balance*. Edward Elgar Publishing, 2017. ISBN: 9781785369353, Chapter 3. Finally, the EU included an obligation to implement technical and organisational measures by design in the draft of the GDPR, later emended and approved. The following section will explain in detail what is prescribed in the final Article 25 on data protection by design and will mention other legal rules on EU data protection law that include a similar provision.

effects and jurisdictional issues might be solved with PbD because protection of privacy may become a default mode in technology, wherever it is used[173]. Thus, embracing PbD might be useful for ensuring more global privacy and data protection[174]. PbD seeks to integrate either privacy or data protection requirements (or both), but each legal framework provides its rules. The jurisdiction where the implementation takes place therefore changes which rules the approach of PbD aims to incorporate. At the same time, technical configurations might be customised from one context to another by following a common approach[175]. The existence of different rules in separate legal frameworks represents a limit to an extended effect. Nevertheless, a common strategy on PbD may be "an outstanding lever for a constructive dialogue" on privacy issues "also at the international level"[176].

Although a legal requirement may be flexible and applicable to various contexts, a broad definition of designing privacy or data protection leads to difficult implementation. A vague design statute does not guide companies, and it might make enforcement arbitrary[177]. It has been argued that technology and law entail different systems of logic: the former operates by on-off rules, while the latter allows interpretative rules[178]. Thus, the translation into code is a challenge[179]. Bridging the gap between legal nat-

173 Ugo Pagallo. "On the principle of privacy by design and its limits: Technology, ethics and the rule of law". In: *European Data Protection: In Good Health?* Springer, 2012, pp. 331–346. ISBN: 9789400729032, p. 333.

174 Everson, "Privacy by design: Taking ctrl of big data", p. 40.

175 As an example, if the technology is implemented in the US, then customisations for the EU market should be made since the rules of information privacy and data protection are different. *See* further Chapter 4. It can also be argued that if the open source movement is accepted a wider social context, technological solutions would circulate easily and they could be customised easily. On the open source movement *see* the initial announcement of the GNU project by Richard Stallman in Richard Stallman. *The GNU project*. <www.gnu.org/gnu/initial-announcement.html>. 1998.

176 This is one of the ways forward for PbD identified by the EDPS in EDPS European Data Protection Supervisor. *Opinion 5/2018, Preliminary Opinion on privacy by design*. 2018, p. 18.

177 *See* Ari Ezra Waldman. "Privacy's Law of Design". In: *UC Irvine L. Rev.* 9 (2018), pp. 1239–1288, pp. 1257–1259.

178 *See* Deirdre K. Mulligan and Kenneth A Bamberger. "Saving governance-by-design". In: *Calif. L. Rev.*
106 (2018), p. 697, p. 710.

179 *See* Spedicato, "Law as Code? *Divertissment* sulla *lex informatica*", pp. 249–250. On the translation problem *see infra*.

ural language and computer language is definitely challenging[180]. Privacy legislation could be vague and ambiguous, while operational commands require precision[181]. Gürses *et al.* investigated the PbD from an engineering perspective. They found that the PbD principle could be too vague a concept for its concrete development[182]. The notions and concepts of privacy and data protection, and the definition of PbD are not uniform: there is a multitude of approaches[183]. A broad and vague definition of PbD hinders any common design methodology[184].

Therefore, *de iure condendo*, and in order to apply PbD, its provision should be framed in a detailed way by the legislator with some criteria for implementation, it should be well drafted and clearly worded, and a thorough legal analysis of applicable legal rules should be performed[185]. The PbD provision should be precise enough to ensure that what is required is sufficiently clear for stakeholders[186]. Theoretically, even the rules that PbD applies should be as specific as possible, but a will be further explained, law is often intentionally vague, and it is open to interpretation and to the balancing of competing interests.

Furthermore, PbD legal requirements should be technologically neutral, but specific solutions must be provided for every technical context. Cavoukian's definition of PbD does not refer to any specific digital technology. Technological neutrality has been defined as the attribute of the rule that does not impose nor discriminate in favour of a particular technology[187]. For the limited current purposes, a regulation is neutral when

---

180 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 283.

181 *See* Bygrave, "Hardwiring privacy", p. 767. According to Diciotti, a provision is ambiguous when the language leads to different meanings (e.g. in the case of polysemy), while it is vague when its meaning (i.e. the norm) is difficult to determine. *See* Enrico Diciotti. *Interpretazione della legge e discorso razionale*. G. Giappichelli Editore, 1999, pp. 360–381.

182 *See* Gürses, Troncoso, and Diaz, "Engineering privacy by design". Other engineering approaches will be discussed in Chapter 5.

183 Tsormpatzoudi, Berendt, and Coudert, "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity", p. 201.

184 Wiese Schartum, "Making privacy by design operative", p. 153.

185 On the need for details *see* Wiese Schartum, *op. cit.*, p. 159. The author pointed out that the detailed framing should be specified by legislators.

186 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, pp. 284–285. The author mentions developers, manufactures and engineers.

187 Mireille Hildebrandt and Laura Tielemans. "Data protection by design and technology neutral law". In: *Computer Law & Security Review* 29.5 (2013), pp.

it is not associated with particular technology artefacts and practices[188]. As regards a general PbD requirement, technology specificity is not relevant. Specific technological solutions will be developed for each context. The legal requirement should be neutral in order to be effective in the future and not be obsolete and limited to a particular rationale. In fact, a principle should be stable and technologically neutral to be applicable for all new cases[189]. Thus, the aim of a neutral regulation is to prevent frequent and unnecessary amendments by legislators. This choice also avoids unjustified interference with the markets of technologies[190]. In some cases, targeted legislation is necessary; accordingly, the target will be the type of mechanism, instead of a specific technology in order to prevent continuous adaptation to new emerging solutions[191].

As a matter of fact, the approach of PbD does not provide fixed solutions and tools[192]. Specific solutions must be provided for each processing operation. As mentioned, technological neutrality is positive[193]. Nonethe-

509–521, p. 510. *See* also Reed, *Making laws for cyberspace*, pp. 189–193, which investigates the meaning of technological neutrality from a historical point of view and for different legal frameworks.

188 *See* Lyria Bennett Moses. "Regulating in the face of sociotechnical change". In: *The Oxford handbook of law, regulation and technology*. Oxford University Press, 2017, pp. 573–596, p. 586. The author discussed the regulatory potential of technology arguing that technology *per se* is irrelevant in justifying regulation (and its timing) because other societal implications influence the necessity to rule. Technology is a regulatory target, but technological specificity, level of regulation and timing are all aspect to be taken into account before framing a rule.

189 Bennett Moses, *op. cit.*, p. 589.

190 *See* Hildebrandt and Tielemans, "Data protection by design and technology neutral law", p. 510. The authors explain that if the rule refers to a particular technology, it will focus on that technology, thereby creating unjustified discrimination and a competitive disadvantage with other tools. It will result in unfair competition.

191 *See ibid.* The example analysed by the authors is the EU cookie legislation. It is worth noting that the authors concluded that the law is never perfectly neutral because it could interfere with the technological design instead of only addressing the use.

192 Tsormpatzoudi, Berendt, and Coudert, "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity", p. 205.

193 *See* also Aurelia Tamó-Larrieux. *Designing for privacy and its legal framework: data protection by design and default for the internet of things*. Law, Governance and Technology Series. Cham, Switzerland: Springer, 2018. ISBN: 9783319986241, pp. 194–195. The author defined regulation as an "enabler" that allows developers to design for privacy. Regulation should be drafted in a technologically

less, a neutral regulation might not guide the developer to the appropriate solution. To this end, the primary rule should remain neutral. As it may not be sufficient to ensure a PbD application in all cases, the legal framework could include specific regulations for distinct technological contexts where this rule should apply[194].

Moreover, privacy by design may improve the effectiveness of the law because design affects every user[195]. PbD seems more effective than other privacy approaches due to its timing: privacy protection is included as a component in the design[196]. PbD may be applicable even towards the emerging technologies that are not specifically regulated by the law yet. PbD may better ensure or almost fully guarantee compliance[197].

Such an approach attaches primary importance to principles and rights. It has been argued that PbD strengthens people's *habeas data*[198]. This principle can be defined as "individual protection against arbitrary action"[199]. PbD empowers individual protection, e.g. the exercise of the data subject's rights, that shall be considered from the beginning of the data processing.

---

neutral and goal-oriented way in order to enable the use of different tools and leave the concrete implementation to a lower level.

194 *See* Article 29 Working Party, Police, and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, p. 15. Article 29 Working Party argued that there could have been cases where a more concrete approach was necessary. Therefore, the legal framework should include more specific provisions for particular technological contexts.

195 *See* Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*; and Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 263. According to Hart, efficiency of law means that the rule is obeyed more often than not. *See* Herbert Lionel Adolphus Hart and Joseph Raz. *The concept of law*. Oxford University Press, 2012. ISBN: 9780199644704, p. 103.

196 *See* Gaia Bernstein. "When new technologies are still new: windows of opportunity for privacy protection". In: *Vill. L. Rev.* 51 (2006), pp. 921–950, pp. 925–926. The author proposed to replace the term "legal intervention" with the term "social shaping". She explained that the early intervention on design shapes social values through technology from a social science point of view.

197 It has been claimed by Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 262.

198 *See* Pagallo, "On the principle of privacy by design and its limits: Technology, ethics and the rule of law", pp. 339–342.

199 *See* Pagallo, *op. cit.*, p. 339. The idea is the digital extension of the writ *habeas corpus*. On the traditional writ of English common law *see* William Blackstone. *Commentaries on the laws of England. Book 1: Of the rights of persons. 1765–1769*. Chicago, Ill.: University of Chicago Press, 1979. ISBN: 0226055361.

It should be stressed that the nature of the rights changes according to the legal frameworks[200].

This advantage may be opposed with the following disadvantage: translating principles, values and rights into machine-readable language is a challenge[201]. PbD requires the translation of rules into engineering and design requirements and business practices. Thus, incorporating PbD means including privacy or data protection considerations in the definition of software and hardware specifications[202]. Legislation is traditionally formulated with language that requires interpretation[203]. Since legal specifications may be inherently generic, the translation or the incorporation in the code is challenging[204]. According to Article 29 Working Party, technological standards could support in defining and specifying requirements[205]. Legal rules may be represented in machine readable forms. As will be reported in Chapter 5, Section 5.3, the Akoma-Ntoso standard – Architecture

200 As regards the EU *see* Section 2.4.8. In the US, rights are granted either by federal law and national law or by common law. For more details, *see* Chapter 4.

201 This challenge was immediately highlighted for the use of DRM in the intellectual property context and for the implementation of the *fair use* doctrine. *See* Roberto Caso. *Digital Rights Management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*. Cedam, 2004. ISBN: 8813252536, pp. 188–191; Samuelson, "DRM {and, or, vs.} the law"; Cohen, "DRM and Privacy"; Timothy K Armstrong. "Digital rights management and the process of fair use". In: *Harv. JL & Tech.* 20 (2006), pp. 49–121; Dan L Burk. "Legal and technical standards in digital rights management technology". In: *Fordham L. Rev.* 74 (2005), pp. 537–573; Burk and Cohen, "Fair use infrastructure for rights management systems". According to this last article fair use allows "the use of otherwise protected material in criticism, comment, parody, news reporting, and similar uses in the public interest". It usually refers to works protected by copyright. Incorporating this rule is a principled approach for engineering privacy by design". In: *Privacy Technologies and Policy. 5th Annual Privacy Forum, 2017*. Springer, 2017, pp. 161–177.

202 *See* Rubinstein and Good, "Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents", p. 1353. On privacy engineering *see* Chapter 5, Section 5.3 of this book.

203 On the challenge of interpretation *see infra*.

204 *See* Woodrow Hartzog and Frederic Stutzman. "Obscurity by design". In: *Wash. L. Rev.* 88 (2013), pp. 385–418, p. 393. The authors proposed a new conceptualisation of PbD, namely *obscurity by design*. The concept of obscurity means that the information on the individual is not in the possession of an observer. The absence of visibility, unprotected access, identification and clarity enhances obscurity, especially in social technologies (*see* at p. 397).

205 *See* Article 29 Working Party, Police, and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, p. 14.

for Knowledge-Oriented Management of Any Normative Texts using Open Standards and Ontologies – provided the schema for the structure and semantic components of digital legislative documents in machine-readable form[206]. Legal ontologies can help to overcome the present challenge by proving methods for representing legal concepts[207].

Translating legal rules into software rules is complex because hard-coding law involves not only representing rules differently, and interpreting provisions or using norms, but also identifying and selecting the applicable and relevant requirements[208]. Courts rule on compliance *ex post* by balancing competing interests and positions and by finding the applicable rules for the concrete case in light of the rule of law, which includes the principles of consistency and legal certainty, and by way of a creative process[209]. According to Koops and Leenes, in the design stage the developer

206 *See* Monica Palmirani and Fabio Vitali. "Akoma-Ntoso for legal documents". In: *Legislative XML for the semantic Web*. Springer, 2011, pp. 75–100; Monica Palmirani. "Legislative change management with Akoma-Ntoso". In: *Legislative XML for the semantic Web*. Springer, 2011, pp. 101–130.

207 *See* Cesare Bartolini, Robert Muthuri, and Cristiana Santos. "Using ontologies to model data protection requirements in workflows". In: *JSAI International Symposium on Artificial Intelligence*. Springer, 2015, pp. 233–248. Generally, on legal ontologies for the privacy domain, see e.g. Valentina Leone, Luigi Di Caro, and Serena Villata. "Taking stock of legal ontologies: a feature-based comparative analysis". In: *Artificial Intelligence and Law* (2019), pp. 1–29; Cleyton Mário de Oliveira Rodrigues et al. "Legal ontologies over time: a systematic mapping study". In: *Expert Systems with Applications* 130 (2019), pp. 12–30. An important ontology that models legal concepts of the privacy domain (GDPR upfront) is PrOnto. *See* Monica Palmirani et al. "Legal Ontology for Modelling GDPR Concepts and Norms". In: *Legal Knowledge and Information Systems. JURIX 2018*. 2018, pp. 91–100; Monica Palmirani et al. "PrOnto Ontology Refinement Through Open Knowledge Extraction". In: *Legal Knowledge and Information Systems. JURIX 2019*. 2019, pp. 205–210; Monica Palmirani et al. "Hybrid Refining Approach of PrOnto Ontology". In: *Electronic Government and the Information Systems Perspective. EGOVIS 20*. Springer, 2020, pp. 3–17. *See* further Chapter 5, Section 5.3.

208 *See* Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", pp. 162–163; Majed Alshammari and Andrew Simpson. "Towards a principled approach for engineering privacy by design". In: *Privacy Technologies and Policy. 5th Annual Privacy Forum, 2017*. Springer, 2017, pp. 161–177.

209 A court interprets the law by way of a creative process. On the creativity of the judicial body with reference to the Italian framework, but which can be extended to a more general and wider debate on laws issued by judges, *see* Roberto Pardolesi and Giorgio Pino. "Post-diritto e giudice legislatore. Sulla creatività della giurisprudenza". In: *Foro it.* col. 113 (parte V 2017). The authors argued

should take into account applicable requirements, case law, legal history, and other relevant legal sources[210]. In a legal system there are general rules, but also domain-specific provisions that could affect data processing. Selecting all the applicable norms *ab initio* is a complex activity even for legal scholars and practitioners[211]. The choice of the sources will impact which norms are implemented, how the system or practice works, and by extension, what is available in the market and what is used for data processing.

The involvement of legal experts and stakeholders during the PbD implementation is essential for taking into account the relevant norms and existing interests. The team of designers must be interdisciplinary. As an example, Guarda and Zannone demonstrated that addressing the mentioned challenge is possible by following step-by-step and strict methods in the presence of legal experts as well as engineers[212]. In addition to this technological implementation, organisational strategies are an important part of the PbD approach that has to be added to the technical part to guarantee compliance with the law.

PbD aims to implement rules, principles and values established by policymakers[213]. The legal sources providing rules for a PbD implementation are firstly the applicable law on privacy and data protection, and secondly

---

that nowadays judicial creativity is inevitable, and is related to interpretation as an exercise of power. On the rule of law *see* e.g. the point of view of the European Court of Human Rights in Geranne Lautenbach. *The concept of the rule of law and the European Court of Human Rights*. Oxford University Press, 2013. ISBN: 9780199671199.

210 Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", p. 166.

211 Legal systems are complex by nature since there are several legal sources. *See* from a legal theory point of view the prominent words of Bobbio in Norberto Bobbio. *Teoria dell'ordinamento giuridico*. G. Giappichelli Editore, 1960, p. 25.

212 *See* the pioneering work of Paolo Guarda and Nicola Zannone. "Towards the development of privacy-aware systems". In: *Information and Software Technology* 51.2 (2009), pp. 337–350.

213 Paraphrasing Hildebrandt, it is arguable that "constitutional democracy entails that enacted law is seen as an instrument to achieve the goals of the democratic legislator". *See* Hildebrandt, "Legal protection by design: objections and refutations", p. 235, where the author proposes the concept of Ambient Law. According to her, this concept is built on privacy by design, value-sensitive design and values in design. Ambient law refers to smart environments and is described as "legal protection by design". It is not a law by technology, but a rule of law which aims to automatically implement legal norms in digital environments. So, PbD aims to achieve these goals.

the special legislation, and, if necessary, case law[214]. Principles could (and should) be used as supplements to the applicable legal requirements[215]. Legal principles could also be promoted for technical standards[216]. However, legal interpretation is flexible and dynamic. It seems difficult to define common principles in different legal frameworks. These are influential concerns from a legal theory point of view, and they will be briefly mentioned here in general terms.

A legal rule can be applied only if it is interpreted[217]. The interpretation has been described as an interaction between the legal source and the interpreter, who is influenced by multiple convictions[218]. As Hart has stressed, the open texture of the legal rule means that a balance between

214 *See* Wiese Schartum, "Making privacy by design operative", p. 163.

215 *See ibid.* Schartum specified that the implementation of the principles should be earlier checked with the applicable and specific law. Contracts could be an additional source of rules.

216 As indicated by Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 589, the Canadian Standards Association Code worked with all the stakeholders – consumers, companies and governments – to define standards that respect principles defined by the law.

217 On legal interpretation *see ex multis* Fabrizio Politi. *Studi sull'interpretazione giuridica*. G. Giappichelli Editore, 2019. ISBN: 9788892120648, which discusses the history of interpretation and examines several approaches; Riccardo Guastini. *Saggi scettici sull'interpretazione*. G. Giappichelli Editore, 2017. ISBN: 9788892109629; Vittorio Villa. *Una teoria pragmaticamente orientata dell'interpretazione giuridica*. G. Giappichelli Editore, 2012; Giorgio Pino. *Diritti e interpretazione. Il ragionamento giuridico nello Stato costituzionale*. Il Mulino, 2010. ISBN: 9788815134271, which focuses on interpreting rights; Vincenzo Omaggio and Gaetano Carlizzi. *Ermeneutica e interpretazione giuridica*. G. Giappichelli Editore, 2010. ISBN: 9788834814239; Joseph Raz. *Between authority and interpretation: On the theory of law and practical reason*. Oxford University Press, 2009. ISBN: 9780199562688; Diciotti, *Interpretazione della legge e discorso razionale*; Robert Alexy and Aleksander Peczenik. "The concept of coherence and its significance for discursive rationality". In: *Ratio Juris* 3 (1990), pp. 130–147; Hans Kelsen. *General Theory of Norms*. Oxford University Press, 1991. ISBN: 9780198252177; Riccardo Guastini. *Problemi di teoria del diritto*. Il Mulino, 1980; Emilio Betti. *Interpretazione della legge e degli atti giuridici*. Giuffrè Editore, 1949. *See* also the point of view of other prominent scholars who focused on the approach called "analisi economica del diritto" in Guido Alpa et al. *Interpretazione giuridica e analisi economica*. Giuffrè Editore, 1982.

218 Sacco, "Legal formants: a dynamic approach to comparative law (installment II of II)", p. 344. On interpretation *see* also the words Raz, *Between authority and interpretation: On the theory of law and practical reason*.

competing interests should be struck case by case[219]. As an example, in the data protection context, legal rules allow flexible application in practice to facilitate the free flow of information and guarantee an adequate and proportionate level of protection[220]. The interpretation preserves the ductility of the legal text in a constantly variable society[221]. In this sense, law can be adaptive to a higher number of contexts[222].

Legal requirements are formulated in such a way to allow flexible application and make implementation challenging[223]. The creativity of the interpreter is related to a legal source, such as statutes and constitutions. Traditionally legal rule can be general or domain-specific, primary or secondary, descriptive or prescriptive, over-inclusive or under-inclusive[224]. The interpreter could also take into account other legal sources, such as case law. Legal interpretation could change over time[225]. The interpreter – i.e. scholars, judges or practitioners – use several categories of arguments and multiple schemes to attribute a meaning to a legal text[226].

---

219 *See* Hart and Raz, *The concept of law*, pp. 124–135. Hart dedicated some brilliant pages to the formalism of law.

220 Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", p. 166.

221 De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 189.

222 *See* the prominent theory of interpretation of Betti in Betti, *Interpretazione della legge e degli atti giuridici*, p. 4, which stresses: "(l'interpretazione) assolve il compito di mantenere sempre in vita, mediante l'intendere, le esigenze di un ordine dell'operare, e precipuamente assolve il compito di conservare in perenne efficienza nella vita di una società, norme, precetti e valutazioni normative, che sono destinati a regolarla o a servirle di orientamento".

223 Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", p. 166.

224 On characteristics of legal rules *see* the perspective on legal theory of Norberto Bobbio. *Studi per una teoria generale del diritto*. G. Giappichelli Editore, 1970.

225 For these last considerations and PbD *see* Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", p. 166; Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 284.

226 On schemes of legal interpretation *see* the research in the field of philosophy of law. *See ex multis* John R Searle. *Expression and meaning: Studies in the theory of speech acts*. Cambridge University Press, 1985. ISBN: 9780511609213; Kevin D Ashley. "Reasoning with cases and hypotheticals in HYPO". In: *International journal of man-machine studies* 34.6 (1991), pp. 753–796; Giovanni Sartor. "A formal model of legal argumentation". In: *Ratio Juris* 7.2 (1994), pp. 177–211; Neil MacCormick. "Argumentation and interpretation in law". In: *Argumentation* 9.3 (1995), pp. 467–480; Kent Greenawalt. "Constitutional and statutory

Some norms cannot be easily embedded by design. Where there is a consensus on the meaning of a rule, or the rule is framed in a detailed way it is less challenging than where there is not[227]. However, PbD does not aim to encode every legal rule and it promotes organisational measures, too.

In addition to this challenge, some conflicts between values are also possible in the design stage and during the interpretation of the requirements. First of all, it is worth noting that there might be concerns about the erosion of practical liberty by the use of technological design and management[228]. Following Brownsword, technological management could pre-

---

interpretation". In: *The Oxford Handbook of Jurisprudence and Philosophy of Law*. 2002. ISBN: 9780199270972; Riccardo Guastini. *Interpretare e argomentare*. Giuffrè Editore, 2011. ISBN: 9788814192951; Fabrizio Macagno et al. "Arguments of interpretation and argumentation schemes". In: *Studies on argumentation and legal philosophy. Further steps towards a pluralistic approach* (2015), pp. 51–80; Douglas Walton, Giovanni Sartor, and Fabrizio Macagno. "An argumentation framework for contested cases of statutory interpretation". In: *Artificial Intelligence and Law* 24.1 (2016), pp. 51–91; Eveline T. Feteris. *Fundamentals of legal argumentation*. Vol. 1. Springer, 2017. ISBN: 9789402411270; Giorgio Bongiovanni et al. *Handbook of legal reasoning and argumentation*. Springer, 2018. ISBN: 9789048194513. In the 1980s, Tarello classified 15 interpretative arguments or speech patterns used by any interpreter with the law. On interpretative arguments *see* Giovanni Tarello. "Argomenti interpretativi". In: *Digesto civ.* (1987), pp. 3–11, which intelligently explains and classifies these arguments. Tarello refers to practitioners who have to persuade a judge and scholars who propose a particular meaning of the law. The arguments are: 1) *argumentum a contrario*; 2) *argumentum a simili*, i.e. analogy; 3) *argumentum a fortiori*; 4) *argumentum a completitudine*; 5) argument of the consistency of legal discipline; 6) psychological argument; 7) historical argument; 8) apagogical argument, i.e. *argumentum ab absurdo* or *reductio ad absurdum*; 9) teleological argument; 10) economic argument; 11) *argumentum ab exemplo*; 12) systematic argument; 13) naturalistic argument; 14) the so-called argument "equitativo"; 15) *argumentum a coherentia* or *analogia iuris*. The same provision may assume different meanings in the arguments used. As an example, the law can be interpreted according to its strictest sense by excluding any extension of the meaning of the terms and any analogy (*ubi lex voluit dixit, ubi tacuit noluit*), or the interpreter can use an analogy or the *ratio legis* included in the preparatory works of the provision by a teleological argument. Tarello provides a specific description for each argument.

227 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 284.

228 Brownsword, "Law, liberty and technology", p. 55. *See* also a similar discussion focused on filtering and the constitutional freedom of speech by Lessig in Lawrence Lessig. "What things regulate speech: CDA 2.0 vs. filtering". In: *Jurimetrics* 38.4 (1998), pp. 629–670.

vent or exclude actions in such a way that the agent is not free to do something, such as break the rules[229]. From a liberal perspective, this condition may diminish moral citizenship since it reduces practical options and, therefore, the autonomy of the agents. In this scenario, Hart's rules of behaviour are challenged. The individual does not have the choice to obey or disobey the rule. PbD thus might create a problem of general legitimacy of the rule because it might be necessary to justify this paternalistic use of technological regulation. Internalising privacy, as in the case of the PbD strategy, indisputably implicates a technological design. It may be supposed that a violation (a disobedience) impacting privacy interests is not practically possible. Brownsword argued that the moral virtue of respecting privacy might disappear, but, at the same level of argument, respecting privacy and data protection might be more urgent than this conceivable impingement on morality[230]. PbD implementation might prevent the possibility of negotiating the practical options[231]. Automation of privacy and data protection rules may impinge the rights to "self-determination" and "informational self-determination" of individuals[232]. Having a right to informational self-determination means that the individuals have the freedom of choice and the opportunity to make their own decisions on what happens with their personal data. It seems that with PbD individuals do not have the opportunity to make their own decisions on what happens with their intimacy or personal data. A response to this argument might be that discussing privacy practices is simply not feasible in the informational relationship performed in the digital market. Actually, the PbD settings take into account users' decisions, keeping them central. According to Cavoukian's seventh principle, the data subject's interests shall be central. If individuals want to give up their rights, they will change the protective default settings with less protective ones.

---

229 Brownsword, "Law, liberty and technology", p. 56. *See* also Roger Brownsword. *Law, Technology and Society: Reimagining the Regulatory Environment*. Routledge, 2019. ISBN: 9780815356462.

230 Brownsword concluded his chapter by highlighting that discussing the impact on liberty is still relevant in the present debate.

231 Again, Brownsword discussed this concern in Brownsword, "Law, liberty and technology", p. 65.

232 *See* Pagallo, "On the principle of privacy by design and its limits: Technology, ethics and the rule of law", p. 339. On the concept of self-determination *see* Theo Hooghiemstra. "Informational Self-Determination, Digital Health and New Features of Data Protection". In: *Eur. Data Prot. L. Rev. 5* (2019), pp. 160–174, pp. 160–162, 171.

Moreover, design choices may create conflicts between values that influence other design choices[233]. The adoption of a particular theory of privacy or data protection configures different frameworks of values[234]. Privacy could acquire different features if conceived in terms of property rights, human dignity, total control, contextual integrity, restricted access or limited control over digital information[235]. Deciding which value should be privileged requires inquiries into the specific context[236]. In addition to privacy principles and values, legal systems establish other principles, inter-

233 Pagallo, "On the principle of privacy by design and its limits: Technology, ethics and the rule of law", p. 338.

234 According to Alpa, in the EU the protection of personal data and privacy involves three directions: the protection of human dignity and self-determination, the protection of the digital market, and the protection of the contracts for digital content that uses personal data. *See* Guido Alpa. "La "proprietà" dei dati personali". In: *Persona e mercato dei dati. Riflessioni sul GDPR*. Wolters Kluver, 2019, pp. 11–33. ISBN: 9788813370510. Therefore, legal rules embed different perspectives and values. In fact, according to Galgano, the GDPR protects both the right of the data subject to self-determination and control over personal data, and the right of the controller to process personal data in the free digital market. *See* Nadia Galgano Zorzi. "Le due anime del GDPR e la tutela del diritto alla *privacy*". In: *Persona e mercato dei dati. Riflessioni sul GDPR*. Wolters Kluwer, 2019, pp. 35–94. ISBN: 9788813370510. Despite the presence of this second soul of the GDPR, it does not conceive data protection in terms of property rights.

235 These are the examples provided by Pagallo in Pagallo, "On the principle of privacy by design and its limits: Technology, ethics and the rule of law", p. 338. One of the most influential privacy conceptions is Nissenbaum's theory of contextual integrity. *See* the prominent paper in Helen Nissenbaum. "Privacy as contextual integrity". In: *Wash. L. Rev. 79* (2004), pp. 119–158. According to the philosopher, the right to informational privacy in terms of contextual integrity is related to the social phenomenon of distinct types of contexts, domains, spheres, institutions or fields (*see* at p. 137). Indeed, "contexts, or spheres, offer a platform for a normative account of privacy in terms of contextual integrity" (*see* at p. 138). Norms of appropriateness and distribution govern each context. Therefore, "whether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination" (*see* at p. 155). This theory highly influenced the US legal framework.

236 *See* Mulligan and King, "Bridging the gap between privacy and design", p. 1017. Mulligan *et al.* argued that Nissembaum's theory of privacy as contextual integrity should guide the design of privacy-protective platforms.

ests and rights that should be balanced in a conflict, such as intellectual property rights and freedom of information.

According to Hartzog, designers should have the freedom to balance values (and principles) case-by-case[237]. In general, the PbD approach does not aim to hinder the design process and its purposes, but seeks to find the right balance. Privacy and data protection are just two of the possible rights and values in place[238]. However, it should be highlighted that balancing rights and values is traditionally a task of the interpreter and judge. Therefore, once again, it should be stressed that a legal expert must be involved in the PbD implementation, which should be the result of interdisciplinary work.

PbD promotes proactive and preventive measures. This proactive approach for privacy represents a significant shift from the traditional one: policymakers directly call on private stakeholders[239]. Enforcing the law generally occurs after a violation (*ex post basis*)[240]. By contrast, technical constraints could prevent actions and auto-execute: the violation of the rule may not occur at all. This *ex ante* approach has efficient effects. For example, an information flow that violates a policy rule can be blocked by a self-executing filter[241]. Hence, *regulation by design* is "immediate": it prevents a forbidden behaviour from occurring with preventive measures[242]. If *regulation by design* is self-executing, the rule might be adjusted more quickly than in the case of law[243].

However, with a proactive approach it could be argued that the State delegates privacy regulation to companies. This private self-regulation may be incompatible with the democratic procedures of law making and law enforcement[244]. In architectural regulation the rule is set by a private party.

---

237 Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, p. 86.

238 On the need to balance data protection with other rights and liberties *see* further Section 2.7.

239 Levin, "Privacy by Design by Regulation: The Case Study of Ontario", p. 119.

240 *See* Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 572.

241 Reidenberg, *op. cit.*, p. 581.

242 *See* Grimmelmann, "Regulation by software", p. 1723.

243 *See* the scenario presented by De Vanna, "The Construction of a Normative Framework for Technology- Driven Innovations: A Legal Theory Perspective", p. 191. Law is slow and requires a great democratic effort.

244 The term "self-regulation" implies several different phenomena. Generally, self-regulation is a creation of a norm by a private entity. *See* further Quarta and Smorto, *Diritto privato dei mercati digitali*, pp. 83–84.

As regards this concern, Tien identified the presence of a transparency problem[245]. The *code* hides the reasons, and the settings are invisible and defined by default[246]. In the *code as law* context, programmers might theoretically become the lawmakers who act at the disposal of the companies[247]. Law making operates in a different way that requires political decisions and is more than a regulation-oriented practice[248]. In addition, the enforcement activity normally requires public bodies, agencies or institutions. Nonetheless, it has been argued that the legislation activity is always public, but may not be "transparent" because of lobbying and influence peddling[249]. As regards *regulation by technology*, governments could participate in the creation process of standards for leading technological development with public goals[250]. As a result, these goals could be recognised as design objectives by the developers. Leenes and Koops suggest that if the government (i.e. the lawmaker) mandates an "enforcement code", such as PbD, there will always be a legitimate rule-making authority[251]. PbD shall be mandated by legislators and established in a specific provision.

PbD may prevent privacy breaches before they happen, but every embedded technical solution is rigid. Therefore, it is necessary to update measures frequently. The first statement is expressed in the Cavoukian's

---

245 *See* Tien, "Architectural regulation and the evolution of social norms", p. 3. On the lack of transparency *see* also Diver and Schafer, "Opening the black box: Petri nets and Privacy by Design", p. 74; Grimmelmann, "Regulation by software", pp. 1734–1738.

246 De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 200.

247 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 283.

248 *See* Serge Gutwirth, Paul De Hert, and Laurent De Sutter. "The trouble with technology regulation: why Lessig's 'Optimal Mix' will not work". In: *Regulating technologies: Legal futures, regulatory frames and technological fixes*. Oxford University Press, 2008, pp. 193–218. ISBN: 9781841137889, p. 196. According to these scholars, Lessig's approach demands the fixation of political ends in regulation. This is problematic for legal practitioners who construct the law in the interplay between their internal obligations and requirements, and the external mobilisations.

249 *See* Tien, "Architectural regulation and the evolution of social norms", p. 9; and Leenes and Koops, "'Code' and privacy-or how technology is slowly eroding privacy", p. 53.

250 Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 591.

251 Leenes and Koops, "'Code' and privacy-or how technology is slowly eroding privacy", p. 51.

first principle: "proactive not reactive, preventative nor remedial". Identifying privacy risks at the initial stage with an assessment is typical for a PbD approach. In addition, according to the Cavoukian's fifth principle, the concept of security plays an important role for PbD. However, it is necessary to bear in mind that the approach *security by design* differs from PbD because designing in security does not entail that privacy has also been embedded[252]. As a matter of fact, addressing data security means that any collection is legitimate as long as data is safe[253]. PbD is a more holistic approach.

Privacy breaches are structural problems of ICTs and represent an opportunity for PbD[254]. Indeed, the increasing number of data breaches reinforces the need for privacy by design[255]. PbD, as previously with PETs, could prevent certain breaches from occurring because they are more difficult to carry out from a technical point of view[256]. The law could also impose liability for breaking technical rules, thereby creating an incentive to design properly[257]. It has been argued that proactivity of PbD both prevents incidents and has the potential to consider privacy opportunities well in advance[258]. A counterfactual analysis on Facebook's and Google's incidents demonstrates that these incidents could have been avoided by the application of accurate design practices[259].

---

252 Kroener and Wright, "A strategy for operationalizing privacy by design", p. 358.

253 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 297.

254 Hustinx, "Privacy by design: delivering the promises", p. 254.

255 *See* the argument in European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, p. 6; EDPB European Data Protection Board. *Guidelines 1/2021 on Examples regarding Data Breach Notification*. 14 January 2021. Version for public consultation. European Data Protection Board, 2021.

256 As regards PETs, *see supra* note no. 146, p. 4. The EU Commission highlighted the importance of the use of PETs for preventing data breaches in a complementary way with the enforceable rules and obligation of the legal framework. European Commission, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*.

257 Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 583.

258 *See* Wiese Schartum, "Making privacy by design operative", p. 155.

259 *See* the interesting analysis by Rubinstein and Good, "Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents'". In the

Despite this promising edge, *regulation by design* as much as any embedded technical solution tends to be rigid. By contrast, *regulation by law* and its interpretation changes over time. It has been highlighted that technical constraints are substantive inalienable rules[260]. They are costly and difficult to change once established, especially if they are deeper in the architecture[261]. Measures should be regularly updated to protect privacy. Privacy threats should be pre-empted, so that implemented solutions are future proof for a long time[262]. On the one hand, PbD is an approach that entails the regulation by code at its core; on the other hand, it is a dynamic approach that requires by default to be updated frequently and also takes into account organisational measures. On this concern, Klitou pointed out that PbD is an ongoing process that needs continuous advancement and re-assessment so as to not fall behind[263].

PbD is evidently a global perspective: it requires both "privacy-by-policy" and "privacy-by-architecture" approaches[264]. Companies usually prefer the former approach for easily complying with the law and shifting the responsibility to users[265]. An appropriate PbD adoption shall balance both approaches[266]. PbD is a full life-cycle approach that combines law and technology[267]. As a consequence, and once again, technical, legal and business stakeholders should collaborate and follow an interdisciplinary approach[268]. It could be difficult and time-consuming, but it is useful and valuable for workable solutions[269]. Clearly, building privacy is critical for developers and not possible in every situation. Although PbD adoption has been strongly encouraged, this approach is not meant to cover every

---

concluding remarks the authors suggested that PbD, when research is performed correctly, protects consumer privacy from breaches and other incidents.

260 Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 572.

261 Reidenberg, *op. cit.*, pp. 582–583.

262 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 312.

263 *See* Klitou, *op. cit.*, p. 325.

264 On these approaches *see* further Chapter 5, Section 5.3.

265 Diver and Schafer, "Opening the black box: Petri nets and Privacy by Design", p. 73.

266 Diver and Schafer, *op. cit.*, p. 75.

267 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, pp. 265, 298.

268 Tsormpatzoudi, Berendt, and Coudert, "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity", p. 2020.

269 *Ibid.*

legal requirement. It is evident that making all data protection provisions automatic is out of reach[270].

PbD requires concrete organisational measures, but companies sometimes lack a knowledgeable organisation. PbD is further dedicated to business and policy levels across the entire organisation[271]. Management should identify tasks and define responsibilities for planning data processing and handling its operations. Concrete measures should be adopted in processes and projects touching every aspect[272]. As noted above, management has a pivotal role in defining data protection as one of the business priorities and objectives. Nevertheless, companies sometimes lack a knowledgeable organisation. In order to implement PbD both legal and technical experts should work together in every organisation[273]. Public authorities, institutions and agencies could lead by example in applying the rules and the PbD approach. According to the EDPS, public administration shall lead by example on data protection by design[274]. Indeed, public services should serve as a role model and be obliged to use only privacy-friendly technologies that are compliant with the law[275].

Furthermore, PbD requires effective measures and less bureaucratic solutions. PbD implementation aims to avoid the "privacy-as-bureaucracy" paradigm. PbD is a process that goes beyond a defined "to-do-list". Measures shall be effective and proportionate to the concrete risks for individuals that are posed by the data processing[276]. Privacy policies or notices should be consistent with the adopted measures and should not be simplistic forms. In order to adopt a PbD approach, investments and allocated resources are indispensable. The costs are often higher in management focus and organisational efforts than in money. Undoubtedly, PbD depends

270 *See* the words in Pagallo, "On the principle of privacy by design and its limits: Technology, ethics and the rule of law", p. 343.

271 *See* Ann Cavoukian. *Privacy by design: From rhetoric to reality*. Information and privacy commissioner of Ontario, Canada, 2014, p. 173.

272 *See ibid.*

273 *See* Wiese Schartum, "Making privacy by design operative", p. 162. This scholar claimes that both legal and software engineering expertise are required for privacy by design.

274 European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 18.

275 This is one of the recommendations in Danezis et al., *Privacy and Data Protection by design – from policy to engineering*, p. 50.

276 As further explained in Section 2.4, this is the approach of the EU.

on the means, resources and skills of the producers or developers[277]. Companies will invest in privacy programs, creating costs that they are usually reluctant to pay[278]. Small and medium enterprises (SMEs) may ignore a PbD requirement because of the implementation cost and the lower risk of being sanctioned[279].

However, these costs could be considered either as deferred costs to protect the company or insurance costs to safeguard against incidents and sanctions[280]. Companies that use a cost-benefit approach might realise that the expected costs represent a future saving, which is a positive investment in economic terms. Actually, a cost-benefit analysis requires reliable data to inform the decision. This data is scarce[281]. Therefore, investment decisions should be informed by other models. On the one hand, as will be explained later, privacy care has a positive impact on consumers' trust and satisfaction in products and services. On the other hand, public funding intervention could allocate some resources to supporting firms through economic incentives. Funding plays an important role in promoting PbD because the market forces are usually not in favour of it[282]. It is worth

277 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 285.

278 Rubinstein, "Regulating privacy by design", p. 1432. On privacy costs before the GDPR *see* the investigation by Alessandro Mantelero. *Il costo della privacy tra valore della persona e ragione d'impresa*. Vol. 24. Giuffrè Editore, 2007. ISBN: 9788814135682, which examines how privacy impacts companies' management from several points of view (e.g. organisation of employees, risk management, service outsourcing), and examines some concrete case studies.

279 *See* Diver and Schafer, "Opening the black box: Petri nets and Privacy by Design", p. 71. These scholars argue that the SMEs are at low risk of being caught. This concern is relevant because according to the European Union Agency for Network and Security (ENISA) SMEs dominate the business landscape of data processing. *See* Giuseppe D'Acquisto and Georgia Panagopoulou. *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Network and Information Security, 2016.

280 A similar argument is used by the US Department of Health, Education & Welfare for supporting the application of the FIPs and their resulting privacy costs. *See* US Department of Health, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records Computers and the Rights of citizens*, p. 45.

281 *See* Rubinstein, "Regulating privacy by design", pp. 1437–1438. The author reported that there is neither reliable data on the benefits of privacy nor data on the costs.

282 *See* this argument in Danezis et al., *Privacy and Data Protection by design – from policy to engineering*, p. 51.

noting that PbD solutions are not necessarily sophisticated but have a range of degrees of sophistication[283]. Therefore, costs may also vary greatly.

PbD may also increase privacy culture in society, but it could be argued that there is a difficulty of comprehension for the layman on this topic. Cavoukian noted that with PbD privacy is not yet considered a compliance issue, but a business issue creating opportunities and a positive paradigm[284]. PbD introduces the opportunity to foster a privacy-first culture[285]. A particular culture of privacy grows within companies and enterprises[286]. Even in the present moment of increased attention on privacy and data protection problems, there is a difficulty of comprehension for the layman on the issues. The lack of technical knowledge and its normative implications have been explained by scholars[287]. People do not have the necessary information to contest a design decision and potentially condemn a wrong implementation. A consumer choice entails awareness and there is a considerable lack of it[288].

Moreover, PbD may contribute to increase trust and confidence in products and services, but in the Information Society there is an information asymmetry and a widespread lack of knowledge on design strategies. It has been claimed that PbD is about trust[289]. Ann Cavoukian usually presents PbD as a tool for restoring trust[290]. Since PbD translates principles into implementation of privacy-protective solutions, it has been argued that fostering trust in ICTs is possible[291]. Trust is an essential component of *healthy relationships and healthy societies*[292]. In the digital economy the

283 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 264.

284 *See* e.g. Cavoukian, "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D", p. 251.

285 Everson, "Privacy by design: Taking ctrl of big data", p. 30.

286 *See* Cavoukian, *Privacy by design: From rhetoric to reality*, p. 223.

287 *See* e.g. Tien, "Architectural regulation and the evolution of social norms".

288 *See* Leenes and Koops, "'Code' and privacy-or how technology is slowly eroding privacy", p. 51. The authors even reflect on the existence of a choice. More considerations on this concern are added to explain the next lines.

289 Everson, "Privacy by design: Taking ctrl of big data", p. 40. This author adds that the adoption of PbD is simply the right thing to do for Big Data.

290 *See* the sixth principle "visibility and transparency", in Section 2.2.

291 Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices", p. 16.

292 *See* Richards and Hartzog, "Taking trust seriously in privacy law", p. 448; and Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, p. 98.

rhetoric of trust and privacy have been widely used internationally[293]. So much, that promoting consumer trust has become a goal for privacy and data protection regulation[294]. Ideally, a data protection framework aims to build trusting relationships between individuals and organisations[295]. Richards and Hartzog proposed a theory of privacy and trust: *privacy matters because it enables trust*[296]. From their perspective, trust is essential for privacy disputes especially in the information relationships[297]. From a digital perspective, where privacy pessimism arises, privacy rules serve constitutional values by creating trust and, therefore, the optimal conditions for intimacy and freedom of expression[298]. In their analysis the two scholars connected the concept of trust with the FIPs and they proposed adding "loyalty" as a foundational concept in privacy law in order to guide privacy discussions. In the EU data protection aims to create trust and boost growth and innovation[299]. As an example, the importance of creating trust due to digital development is highlighted in Recital 7 of the GDPR: trust is important for allowing the development of the digital economy across the EU market[300]. According to the European Commission, protective technology, such as PETs, could have a positive impact on consumers because people are more certain that data are managed in a proper way[301]. Since PbD is a particular approach to privacy, it can set foundation for trust over technology. According to the European Data

293 Kenneth A. Bamberger and Deirdre K. Mulligan. "Privacy on the Books and on the Ground". In: *Stan. L. Rev.* 63 (2010), pp. 247–315, pp. 280–281.

294 *See* Bamberger and Mulligan, *op. cit.*, p. 282. These authors observe that in the US privacy is associated with trust both for and against the creation of a regulation. However, the Federal Trade Commission's agenda was always dedicated to consumer protection in order to foster confidence and trust.

295 In this context the term organisation indicates both private parties (e.g. companies, firms) and public bodies (e.g. public administration, authorities).

296 Richards and Hartzog, "Taking trust seriously in privacy law", p. 447.

297 The two authors noted that trust is also essential for any commercial relationship in every context. *See* Richards and Hartzog, *op. cit.*, p. 452.

298 Richards and Hartzog, *op. cit.*, p. 456.

299 Hijmans et al., *The European Union as guardian of internet privacy*, p. 320.

300 Recitals set out the rationales of the creation of the uniform framework. In particular, the part mentioned states that (rapid technological) "developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market".

301 *See supra* note no. 146. The EU Commission argued that greater respect for data protection rules has a trust impact on services based on the processing of personal data, such as e-health. European Commission, *Communication from*

Protection Supervisor (EDPS), PbD is a key tool for generating individual trust in ICTs[302]. Technologies should be reliable and secure for generating trust and PbD is a positive solution to achieve this goal. Thus, PbD could be seen as an example for enhancing trust in data protection law and for creating economic incentives in the EU[303].

Although it has been claimed that PbD could boost trust, it should be noted that in society there is an information asymmetry between different parties and a widespread lack of knowledge on design strategies. The information asymmetry exists between the digital environment and the user who acts without knowing, and controlling, the mechanisms in the background[304]. Scholars have argued that the information asymmetry is a kind of a "computational divide" where the user does not have any control on the digital environment[305]. This unprecedented asymmetry operates in knowledge and power[306]. Even in a "privacy as control" scenario, one risk is the creation of a "smoke screen" that misleads users' choices[307]. Consumers should have the opportunity to exercise an informed choice when purchasing products and using digital technology. More information and

---

*the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*.

302 *See* European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, p. 4.

303 *See* Hijmans et al., *The European Union as guardian of internet privacy*, p. 320. The author suggests in his book that PbD should have been an instrument in economic policies of the EU. Moreover, it can create more trust in data protection law (*see* at p. 599).

304 *See* De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 187. Asymmetry is a market failure. *See* the useful explanation in Quarta and Smorto, *Diritto privato dei mercati digitali*, pp. 67–69.

305 De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 187. On the lack of consumer understanding *see* also Rubinstein, "Regulating privacy by design", p. 142. This information asymmetry even operates between the private and public sectors since authorities use ICTs, algorithms, data (and Big Data) to make decisions. *See* the interesting analysis by Maria Cristina Cavallaro and Guido Smorto. "Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo". In: *Federalismi.it* 16 (2019), pp. 2–22.

306 Shoshana Zuboff. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books, 2019. ISBN: 9781610395694, p. 17.

307 *See* the criticism by Paul M. Schwartz. "Beyond Lessig's code for internet privacy: cyberspace filters, privacy control, and fair information practices". In: *Wis. L. Rev.* 2000.4 (2000), pp. 743–788, pp. 760–762.

transparency tools might overcome this disadvantage[308]. However, enhancing individuals' control might not be sufficient and, once again, a global approach is more advisable. PbD could increase consumers' satisfaction because it empowers them to control their privacy and personal data behind the screen[309].

Additionally, PbD has an impact on business because companies have the opportunity to use new technologies and adopt innovative internal processes and policies[310]. The quality of the design is thus a means for developing value for business[311]. A commitment to PbD could also be considered a competitive advantage that enhances business reputation[312]. However, collecting and commercialising personal data are the core business of many companies. The processed data has a substantial economic value, and is regarded as a business asset by firms[313]. Data is used to target or offer products and services, provide advertising in the online

308 *See* European Commission, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, pp. 8–9. In the EU Commission's Communication on PETs the authority suggested that "simple and understandable information about possible technological tools to protect privacy must thus be provided to the user" and, therefore an "increased use of PETs and increased use of e-services which incorporate PETs will in turn mean economic reward to the industries using them, and may result in a snowball effect, encouraging other companies to pay greater attention to respecting the data protection rules".

309 Rubinstein, "Regulating privacy by design", p. 1422.

310 Anna Romanou. "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise". In: *Computer law & security review* 34.1 (2018), pp. 99–110, p. 102.

311 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 281. According to the author, this statement is demonstrated in countless examples.

312 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*,
p. 19. *See* also Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices"; Massimo Farina. *Il cloud computing in ambito sanitario tra security e privacy*. Giuffrè Francis Lefebvre, 2019. ISBN: 9788828817550, p. 21.

313 *See* the prominent analysis on the economics of privacy in Alessandro Acquisti, Curtis Taylor, and Liad Wagman. "The economics of privacy". In: *Journal of economic Literature* 54.2 (2016), pp. 442–492, p. 444; and the empirical study of Kenneth A. Bamberger et al. "Can you pay for privacy? consumer expectations and the behaviour of free and paid apps". In: *Berkeley Tech. LJ* 35 (2020), pp. 328–365.

ecosystem or is traded with other third parties[314]. So, it has been argued that the PbD approach may collide with the common logic of the digital economy, which incentivises the so-called "monetarization of monitoring" of end-users' data[315]. As an example, it is evident that the collection of personal data on social networks platforms is massive. A great amount of data is uploaded by users, and is also processed and inferred by companies and intermediaries, sometimes in an unsecured way[316].

Scholars classify some business models that represent approaches for monetising data. According to Elvy, the "pay-for-privacy" (PFP) approach requires the payment of a higher fee or price to avoid data collection and advertising[317]. Secondly, the "personal data economy" (PDE) approach attributes data ownership to individuals by empowering their control over information[318]. The former approach is less common than the latter, but

314 Acquisti, Taylor, and Wagman, "The economics of privacy", p. 444.

315 Bygrave, "Hardwiring privacy", p. 763.

316 A paradigmatic case on this issue is the Cambridge Analytica scandal of 2018. In this scandal the amount of data collected by a particular business model is crucial. Basically, this corporation developed a method to "micro-target" individual consumers or voters on Facebook with messages aimed at influencing their behaviour. *See* Jim Isaak and Mina J. Hanna. "User data privacy: Facebook, Cambridge Analytica, and privacy protection". In: *Computer* 51.8 (2018), pp. 56–59, p. 56. It is conceivable that this system influenced the US presidential elections of 2016. A data breach of 50 million profiles occurred and was revealed to *The Guardian* by whistleblower in 2018. *See* Carole Cadwalladr and Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". In: *The Guardian* 17 (2018), p. 22. CEO Mark Zuckerberg was asked to testify before the European Parliament and the US Congress. The European Parliament adopted the Resolution of 25 October 2018 "on the use of Facebook users' data by Cambridge Analytica and the impact on data protection" (2018/2855(RSP)). The EDPS released an opinion "on online manipulation and personal data". *See* EDPS European Data Protection Supervisor. *Opinion 3/2018, EDPS Opinion on online manipulation and personal data*. 2018. On December 6, 2019 the FTC filed a complaint against Cambridge Analytica, LLC. Ten days later, the final approval of a settlement with the corporation was granted by the authority. On this file, *see* at <www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter>. Last accessed 06/10/2021.

317 *See* Stacy-Ann Elvy. "Paying for privacy and the personal data economy". In: *Colum. L. Rev.* 117 (2017), pp. 1369–1460, p. 1373. The author explain that companies usually provide discounts to consumers who give their consent to data collection and advertising.

318 Elvy, *op. cit.*, pp. 1374–1375. The author pointed out that this control can be illusory because of the lack of consumers' understanding of the privacy implications.

neither are widespread. The "data-as-payment" model, on the other hand, is very common. Consumers/users provide their data in exchange of a free product or service. This third model is used by big companies such as Google and Facebook to create an imperfect transaction where data has more value than the product or service provided[319]. Overall, these economic models raise concerns for privacy and, therefore, the PbD approach struggles against the logic of the digital market[320].

The market dynamics surrounding personal data have been defined as "surveillance capitalism" by prominent Harvard scholar Shoshana Zuboff[321]. Internet companies (e.g. Google) are surveillance capitalists that operate with the logic of information accumulation. The so-called "behavioural data" of users are extracted at large scale and then analysed. Only a small part of collected information is used for service improvement. The surplus is sold to other companies for advertising purposes and to create future market-based behavioural information[322]. The business model is described with an economic theory[323]. So, the different logic of minimisation and privacy protection seems inevitably at odds with the surveillance

319 Elvy, *op. cit.*, pp. 1384–1387.

320 It is interesting to note that sharing economy companies create the same privacy concerns. Even though they charge a price for their services, the narrative of manipulation remains the same. *See* e.g. Ryan Calo and Alex Rosenblat. "The taking economy: Uber, information, and power". In: *Colum. L. Rev.* 117 (2017), pp. 1623–1690, pp. 1648–1654. This article presents a case study on Uber. On law, sharing economy and digital markets *see* Quarta and Smorto, *Diritto privato dei mercati digitali*. This book explains the phenomena of the digital economy, and the effects on work and competition.

321 *See* the prominent book of Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, p. 15. On this topic *see* also the analysis by Quarta and Smorto, *Diritto privato dei mercati digitali*, pp. 173–176. The authors point out that individuals are manipulated in surveillance capitalism. People are unaware of their choices.

322 *See* Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. In particular, *see* Chapter 2. The author explains the history of the digital revolution in comparison with Ford's inventions. Zuboff describes in detail Google's history and business model. This company collects data from Internet searches.

323 In Zuboff's framing: "The summary of these developments is that the behavioural surplus upon which Google's fortune rests can be considered as surveillance assets. These assets are critical raw materials in the pursuit of surveillance revenues and their translation into surveillance capital. The entire logic of this capital accumulation is most accurately understood as surveillance capitalism, which is the foundational framework for a surveillance-based economic order: a surveillance economy" (*see* at p. 93).

model[324]. However, the same scholar mentions privacy by design in the vital and necessary accomplishment of a regulatory framework that might challenge this new capitalism. In fact, Zuboff argues that the EU legal framework might challenge the dynamics of surveillance capitalism with the rules on data protection[325].

The more people are aware of the processing activities, the more they will be protected, and the information asymmetry might be reduced within its power asymmetries. At the same time, it has been claimed that privacy regulation alone is insufficient to change this current capitalist model[326].

It may be also argued that with PbD there is a business opportunity for certifications and standards, but certification does not automatically mean compliance with the law. Certification is defined as a "conformity assessment activity"[327]. It is usually issued by an entity after a certification procedure. Certification might or might not be based on legislation. It is an opportunity because it has a voluntary basis. Certification can assist data controllers in demonstrating compliance with legal obligations. Moreover, certification can increase confidence in products and services[328]. Indeed, certification can play a significant role for PbD because the details of this complex approach can be defined by intermediaries between the regulator and the regulated, which may be appointed by data protection authorities[329]. An independent and standardised certification scheme on PbD could determine the validity and adequacy of solutions[330]. One example

---

324 As regards the relationship of surveillance capitalism to privacy, *see* Chapter 6 of the book, where the scholar perfectly describes the scenario of the mentioned disadvantage: internet companies are not interested in privacy protection because it is dangerous for their business model, which is at its core based on data (such as a new oil).

325 *Ibid.*, *see* Chapter 17 of the same book. According to the Harvard scholar, only timing and society will show if the economic model can change thanks to a new advanced regulatory framework such as the EU one.

326 Quarta and Smorto, *Diritto privato dei mercati digitali*, p. 176.

327 *See* ENISA European Union Agency for Network & Information Security. *Recommendations on European Data Protection Certification*. European Union Agency for Network and Information Security, 2017, p. 9.

328 *See* the argument used in Danezis et al., *Privacy and Data Protection by design – from policy to engineering*, p. 16.

329 *See* Levin, "Privacy by Design by Regulation: The Case Study of Ontario", p. 156. As will be explained in Section 2.5.3, this is the approach of the EU framework.

330 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 309.

of PbD certification is the one offered by the PbD Centre of Excellence at Ryerson University in Ontario[331]. This certification is based on FIPs[332].

Furthermore, standards are means for complying with the law. Technical standards can also be useful for data protection authorities because they represent a first point of reference for compliance-checking[333]. Standardisation is a form of regulation[334]. A standard is a self-regulation which is more flexible than a regulation subject to a democratic legislative process[335]. An international standard on PbD in currently under development by a technical committee of ISO[336]. Although certification and standards are widely useful, they do not automatically mean compliance with the law. Compliance is verified by the courts and by data protection authorities. In most cases certification does not reduce the liability of subjects[337]. Moreover, as with self-regulation, certification and standards are usually mar-

331 *See* Ann Cavoukian and Michelle Chibba. "Privacy seals in the USA, Europe, Japan, Canada, India and Australia". In: *Privacy and data protection seals*. Springer, 2018, pp. 59–82. ISBN: 9789462652286, p. 77. This certification programme is directed by Ann Cavoukian in collaboration with Deloitte.

332 *See* European Union Agency for Network & Information Security, *Recommendations on European Data Protection Certification*, p. 18. In this report the agency analyses certification, which does not signify compliance with a specific law, but uses Cavoukian's approach. Certification follows an important best practice: the entity that examines the product or service (i.e. Deloitte) is different from the entity that issue the certification (i.e. the Privacy by Design Centre of Excellence at Ryerson University).

333 Irene Kamara. "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'". In: *European Journal of Law and Technology* 8.1 (2017), pp. 1–24, p. 2.

334 In the EU there is a specific regulation on European standards. *See* Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, O.J. L. 316, 14.11.2012.

335 *See* Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 197.

336 *See* project ISO/PC 317 "consumer protection: privacy by design for consumer goods and services" at <www.iso.org/committee/6935430.html>. Last accessed 06/10/2021. Cavoukian mentions the importance of this standard in Cavoukian, "Understanding How to Implement Privacy by Design, One Step at a Time".

337 As will be explained in Section 2.5.3, certification does not avoid the liability of the data controller under the GDPR, but it will be taken into account by the DPA during the investigation and the proceedings.

ket-driven and, so, unsupervised by the authorities. Costs are high in the case of international certifications. Therefore, SMEs could be discouraged from paying such expensive costs to get certified. Copyrights on standards have transformed initial "public goods" into fragmented "club goods"[338]. However, it has been argued that both regulation and self-regulation are needed in a legal system[339].

PbD requirement incentivises the development of new privacy-friendly technologies from the beginning[340]. This is the aim of Cavoukian's seventh principle. In this sense, PbD has proven to be a useful innovation in the design community[341]. Since the approach is easily applicable to new technologies, adapting the existing solutions is not always feasible. As a result, strategies for the PbD implementation should be elaborated case-by-case after a balance between competing interests. Sometimes, the easier choice is to change technologies.

*Regulation by technology* is a form of control. It has been claimed that a new ethics of responsibility should revise some legal categories and inspire regulatory solutions[342]. Authorities might become involved in unusual types of activities, such as promoting technical standards[343]. The call for an ethical foundation in technology has a broad scope. PbD is arguably an unprecedented opportunity to boost respect for ethics in technology[344]. In this controlled scenario, there will be barriers to innovation. According to Quarta and Smorto, since the 1970s the word "innovation" has substituted the word "progress"[345]. An innovation is a technological novel creation

338 *See* this critique in Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 197.

339 *Ibid.*

340 Hijmans et al., *The European Union as guardian of internet privacy*, p. 296.

341 Hartzog and Stutzman, "Obscurity by design", p. 391.

342 *See* De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective", p. 200. The author discusses design theory and argues for a regulation by law over technology.

343 In this sense, as mentioned above, an example is the collaboration between the Canadian Standard Association Group and the Government of Canada. *See* for lobbying information <lobbycanada.gc. ca/app/secure/ocl/lrs/do/clntAddr?cid=5290&sMdKy=1382894400185>; and for all the other information <www.csagroup.org/about-csa-group/>. Last accessed 06/10/2021.

344 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 21.

345 *See* Quarta and Smorto, *Diritto privato dei mercati digitali*, pp. 29–30.

that contributes to meeting society's recognised needs, i.e. it brings a better change by offering new and creative ways of responding to social needs[346].

The approach of privacy by design indirectly aims to control the development process of products and services in order to improve the protection of privacy and personal data. Studies reported by Lieshout show that privacy has potential negative consequences for innovation[347]. This scholar reports some empirical studies on the impact of privacy on business, concluding that the latter promotes innovation to the detriment of privacy. Interestingly, in this study PbD has been considered an innovative practice. On the one hand, proactive technological regulation, such as PbD, may stifle innovation because it requires anticipating any potential misuse and limits the developer[348]. On the other hand, new and creative solutions should be implemented in the market for applying PbD. Hence, the interpreter may evaluate PbD as an innovative approach for its own sake. Compromise is always necessary when designing with privacy in mind[349].

The last line of Table 2.1 indicates that PbD aims to implement user-centric technologies, but there might be increasing costs for access to digital technologies. PbD is pivotal for technological development, especially where specific data protection concerns arise[350]. Within PbD users should be considered upfront. They are supposed to have more control in the default settings. According to Cavoukian, user-centricity means designing for users and anticipating their privacy perceptions, needs, requirements, and default settings[351]. Generally, the design is user-centric when privacy settings are regulated towards users' needs. Engineering assigns a partially different meaning to the term user-centric. User-centred development (UCD) represents an engineering approach to software design. This is an

346 Quarta and Smorto, *op. cit.*, p. 30.

347 *See* Marc Van Lieshout. "Privacy and Innovation: From Disruption to Opportunities". In: *Data protection on the move*. Springer, 2016, pp. 195–212. ISBN: 9789401773768, pp. 204–206. The author uses the OECD's definition of innovation: something new to a firm, to the market and to the world.

348 *See* Hildebrandt and Tielemans, "Data protection by design and technology neutral law", p. 519. This study discusses the DPbD requirement in relation to the technological neutrality and its objectives (compensation, innovation and sustainability).

349 Everson, "Privacy by design: Taking ctrl of big data", p. 32.

350 *See* Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", pp. 104–109. The contexts analysed by the author are biometric technology, e-health and video surveillance.

351 Cavoukian, *Privacy by design: From rhetoric to reality*, p. 42.

interactive methodology that involves the user in the design process for giving input and feedback[352]. However, in the former sense, the interface and the default settings are of primary importance. In a prominent study, the French Data Protection Authority (CNIL) highlighted the need for regulation of design and architectures of choice for interfaces conceived in a broad sense[353]. According to the CNIL, interface design is crucial[354]. Indeed, interface design plays an important role in the effective enforcement of regulation[355]. User choices are directed through technological design and its interface. As a matter of fact, interfaces could use heuristics and biases to nudge users to act in certain ways[356]. A requirement for PbD can discourage companies from creating nudges. The legal concept of transparency is eminently user-centric, and is thus a central principle for achieving PbD[357]. User-centric default settings are also important because individuals usually stick with the existing default choice. This is the so-called "*status quo bias*"[358]. An appropriate default setting could improve this status. It is then arguable that in the future there might be increasing costs for access to digital technologies. Companies will invest in the development of compliant products and services and competition issues might impinge on the open sharing of solutions[359]. Therefore, goods and services may increase in price. However, policymakers could encourage companies

352 On this process *see* Michael DeBellis and Christine Haapala. "User-centric software engineering". In: *IEEE Expert* 10.1 (1995), pp. 34–41.

353 *See* CNIL Commission Nationale de l'Informatique et des Libertés. *La forme des choix. Données personnelles, design et frictions désirables. Cahier n. 6*. 2019, p. 39.

354 *See ibid.* The CNIL observes that "Le design des interfaces – entendu au sens large, depuis l'architecture du service jusqu'à la mise en forme des dispositifs d'information et de consentement – est bien un médium essentiel par lequel se joue la mise en application réelle du règlement et la conformité des services dans cet espace contraint".

355 According to CNIL, the regulation of architectures of choice will represent one of the most important areas of regulation in the next few years, even beyond mere data protection and privacy issues.

356 *See* Alessandro Acquisti et al. "Nudges for privacy and security: Understanding and assisting users' choices online". In: *ACM Computing Surveys (CSUR)* 50.3 (2017), pp. 1–41, p. 2. The authors explained in detail the phenomenon of nudge.

357 Commission Nationale de l'Informatique et des Libertés, *La forme des choix. Données personnelles, design et frictions désirables. Cahier n. 6*, p. 40.

358 *See* Hartzog and Stutzman, "Obscurity by design", p. 412.

359 *See* Wiese Schartum, "Making privacy by design operative", p. 173.

through public funding or other mechanisms to adopt appropriate measures and high standards, and effective policies[360].

The conflict between advantages and disadvantages shows that PbD is a promising principle with many significant concerns. It is challenging to find the right balance between edges and challenges. Despite all limitations, as Hartzog and Stutzman wrote, "it is clear that privacy by design is a useful way of addressing the privacy challenges that technology designers face"[361]. Stakeholders require tangible guidance on designing for privacy[362]. PbD could serve as a bridge between stakeholders – e.g. lawmakers, practitioners, engineers – and as a useful option for balancing competing interests[363].

To achieve these goals and move to implementation, it is necessary to internalise the approach and collaborate among disciplines. Regulation by design should be combined with procedural strategies. Hard and soft privacy should both be considered during implementation[364]. This is the approach of the European Union.

The EU legal framework tried to modernise the rules on data protection in 2016[365]. Indeed, a legal and enforceable obligation to adopt technical and organisational measures by design has been established with the new Regulation. The next section is dedicated to the analysis of this central legal requirement.

---

360 Reidenberg, "Lex informatica: The formulation of information policy rules through technology", p. 589.

361 These are the words of Hartzog and Stutzman, "Obscurity by design", p. 392.

362 Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 197.

363 Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, pp. 323, 328.

364 On the definition of hard privacy and soft privacy *see* Daniel Le Métayer. "Whom to Trust? Using Technology to Enforce Privacy". In: *Enforcing Privacy*. Springer, 2016, pp. 395–437. ISBN: 9783319250472, p. 397. The dissimilarity is related to a different trust assumption. The former identifies the strong approach which does not put trust in the data controller, while the latter trusts the data controller because it assumes that the data subject loses control over data and the controller deserves trust. *See* further Chapter 5, Section 5.3.

365 *See* Christopher Kuner et al. *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 5–43.

## 2.4 Deconstructing Article 25 of the GDPR

With its full applicability on 25 May 2018 the GDPR became the uniform and harmonised legal framework for regulating and protecting personal data in the EU. This section will analyse the legal basis for the principle of data protection by design.

The GDPR incorporates a general provision for data protection by design in the EU legal framework. This requirement and the provision on data protection by default are the most innovative and ambitious norms of the GDPR and they impose qualified duties on data controllers[366]. They represent an attempt to bring people and their rights back to the centre[367]. Basically, the Regulation states that in order to be able to demonstrate compliance with its norms the data controller shall adopt internal policies and implement measures which meet the principles of data protection by design and data protection by default[368].

Controllers, both private and public entities which process personal data, shall implement appropriate technical and organisational measures that achieve data protection principles in an effective manner and integrate the necessary safeguards into the processing at the time of the determination of the means for processing and at the time of the processing itself. They have to take into account some criteria, which are the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the same processing operations.

Therefore, technical and organisational measures are not defined by the law, but they must be appropriate and effective in relation to the data processing operations[369]. The controllers can demonstrate compliance

366 *See* Lee A Bygrave. "Data protection by design and by default: deciphering the EU's legislative requirements". In: *Oslo Law Review* 4.2 (2017), pp. 105–120, pp. 107, 114.

367 The expression is the translation of the words used by Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*, p. 29.

368 *See* Recital 78 GDPR and Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 168.

369 *Ibid.*

through an approved certification mechanism. Article 25 is one of the best examples of the "accountability" approach[370].

Article 25(1), the legal basis for DPbD, reads as follows:

> "1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

Article 25(1) establishes the DPbD obligation that was initially defined in the Proposal of the GDPR in Article 23, later emended in the legislative process[371]. According to Bygrave, the differences between Article 25 and

---

370 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*. Previously, *see* also in European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, p. 19.

371 Art. 23, par. 1, Proposal *see* note no. 129, reads: "1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services. 4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). According to Recital 130 of the Proposal, the European Commission should have the implementing power for defining

Article 23 of the Draft are the followings. Article 25 specifies two examples of measures and additional considerations to take into account, and includes the certification scheme[372]. As regards the factors, the increase in parameters completes the concrete evaluation of processing operations, but also complicates it by not explicitly providing for a hierarchy between them[373]. The additional important criteria are "the nature, scope, context and purposes of processing" and "the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". The timing is equal in both of the provisions, but Article 25 adds the reference to the data protection principles, which must be safeguarded in an "effective manner". Moreover, the European Parliament deleted the third and fourth paragraphs of Article 23 where the EU Commission would have been empowered to adopt: 1) delegated acts for specifying further criteria and requirements for appropriate measures and mechanisms, also applicable across sectors, products and services; 2) technical specifications for the requirements and standards form in relation to the responsibility of the controller. These delegated acts and standards would have been very useful for data controllers and practitioners in general[374]. Undoubtedly, these specifications would have been less binding, but they could have been modified frequently according to the technical state-of-the-art. This choice now leaves the floor to the market for standards and measures[375].

Article 25 has to be interpreted on a case-by-case basis because it contains a general provision with lots of criteria to be taken into account relating to specific data processing. The wording "taking into account" relates to a thought process that has to consider different elements and

---

standards forms in relation to the responsibility of the controller to data protection by design and by default".

372 *See* Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements", p. 114. This scholar also argued that Article 25 applies to processors, but the drafted version does not. As regards this aspect, *see* Section 2.4.1.

373 *See* Federico Sartore. "Privacy-by-design, l'introduzione del principio nel corpus del GDPR". in: *Circo- lazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*. Giuffrè Francis Lefebvre, 2019, pp. 295–307. ISBN: 9788828809692, p. 299.

374 *See* Bincoletto, *La privacy by design. Un'analisi comparata nell'era digitale*, p. 136.

375 *See ibid.*

multiple scenarios with specific risks[376]. The requirement does not provide a "one-size-fits-all" approach, but it leaves flexibility to data controllers[377]. Due to the generality and flexibility, this article constitutes the "architrave of the duties" of the data controller[378]. The provision contains an obligation to act, and in particular an obligation of results[379]. Actually, Article 25 follows Article 24, which is dedicated to the responsibility of the controller[380].

In general terms, it seems that the language of the text is vague and complex[381]. Commentators have argued that the provision offers little clarity and its legalese obscures the meaning[382]. However, this Article is a

376 *See* Lina Jasmontaite et al. "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR". In: *Eur. Data Prot. L. Rev.* 4 (2018), pp. 168–189, p. 177.

377 *See* Levin, "Privacy by Design by Regulation: The Case Study of Ontario", p. 152.

378 *See* Giuseppe D'Acquisto et al. *Intelligenza artificiale, protezione dei dati personali e regolazione*. Torino: G. Giappichelli Editore, 2018. ISBN: 9788892112575, p. 107.

379 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 173.

380 Article 24 GDPR: "1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller". On Article 24 *see* Christopher Docksey. "Chapter IV Controller and Processor (Articles 24–43). Article 24. Responsibility of the controller". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 555–570. ISBN: 9780198826491.

381 *See* Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements", p. 117.

382 *See* Ira S. Rubinstein and Nathaniel Good. "The trouble with Article 25 (and how to fix it): the future of data protection by design and default". In: *International Data Privacy Law* (2019), pp. 1–20, p. 2; Ari Ezra Waldman. "Data Protection by Design? A Critique of Article 25 of the GDPR". In: *Cornell Int'l L.J.* 53 (2020), pp. 147–167.

"conversation-starter" for all stakeholders because it seeks to increase the effectiveness of the protection set by the GDPR[383].

The requirement is technically neutral so as to prevent the risk of circumvention. In fact, Recital 15 GDPR explains that the protection of natural persons should be technologically neutral and should not depend on the techniques used in the processing[384]. The GDPR is neutral by design. A technologically neutral requirement avoids a circumventing case where a different technology is used than the one forbidden by the law[385]. Indeed, as noted above, the requirement will be applied "in the long term to various contexts independently from the technology progression"[386].

As far as this study is concerned, it is relevant to highlight that even Article 17 of Data Protection Directive 95/46/EC (DPD) referred to technical measures, but the emphasis was on security concerns[387]. The Directive did not contain an explicit requirement for privacy or data protection by

383 For the expression "conversation-starter" *see* Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements", p. 120. For the argument *see* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*. This argument is pointed out in the executive summary of the Opinion.

384 *See* Recital 15 of the GDPR.

385 *See* Kamara, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", p. 10.

386 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 169.

387 *See* e.g. Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements", p. 108; and Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 84. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995. This Directive is no longer in force because it has been repealed by the GDPR. The text of Article 17(1–2) DPD on "Security of processing" stated: "1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures".

design, but the provision of Article 17 indirectly demands the implementation of measures that prevent unlawful data processing[388]. According to Recital 46 of DPD, the timing of these measures is the same as Article 25[389]. Nonetheless, this indirect provision did not attribute the powers of enforcing an implementation by design to the authorities[390]. Therefore, in 2010 the EDPS urged the Commission to propose a general provision on PbD and to promote this principle at the policy level[391].

It could be argued that Article 25 has other legal antecedents and that it is not the only provision in the EU framework on data protection by design[392].

---

388 *See* European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, p. 7; and Koops and Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", p. 164. According to Koops, Article 17 is a clear example of a system level requirement that aims to protect personal data against accidental or unlawful destruction or accidental loss.

389 Recital 46 DPD refers to "the time of the design of the processing system and the time of the processing itself".

390 *See* European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, p. 7.

391 *See* European Data Protection Supervisor, *op. cit.*, pp. 8, 21.

392 A long analysis on the legal antecedents is provided in Bincoletto, *La privacy by design. Un'analisi comparata nell'era digitale*, pp. 149–165. It is worth highlighting that the antecedents were mainly soft laws (e.g. recitals where the rationale of the norm is expressed), or communications of the EU Commission. As an example of a legal requirement, Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 – on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) – establishes a privacy by design requirement for the EU Commission. Article 5(1) states that: "the Commission shall develop the ODR platform and be responsible for its operation, including all the translation functions necessary for the purpose of this Regulation, its maintenance, funding and data security. The ODR platform shall be user-friendly. The development, operation and maintenance of the ODR platform shall ensure that the privacy of its users is respected from the design stage ('privacy by design') and that the ODR platform is accessible and usable by all, including vulnerable users ('design for all'), as far as possible". This Regulation is in force. Moreover, as regards soft law, Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 – on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation') – specifies at Recital 7 that the system follows the privacy-by-design principle of

As regards the other norms, it is first relevant to mention Directive 680/2016 and Regulation 2018/1745[393]. The former law was approved in the EU data protection reform package along with the GDPR[394]. The Data Protection Directive for Police and Criminal Justice Authorities sets the rules for "the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data"[395]. According to Article 20, the Directive indicates that the Member States shall provide an obligation of DPbD for data controllers[396]. The latter represents the legislation applicable for data

offering a considerably higher level of protection and security. This Regulation is also in force.

393 All the EU-related provisions are also classified by Lee A. Bygrave. "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 571–581. ISBN: 9780198826491.

394 The Directive has applied since 5 May 2016 and the Member States had to incorporate it into their national law by 6 May 6 2018.

395 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J. L. 119, 4.5.2016.

396 Article 20 Directive (EU) 2016/680: "Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects". Interestingly, this norm does not refer to the certification mechanism. The Eur-Lex portal lists the national transpositions that had to take into account Article 20 (*see* <eur-lex.europa.eu/>). As an example, the Italian act contains a specific provision on DPbD, borrowing the text of Article 25 GDPR almost entirely. *See* Article 16, D.Lgs. 18 maggio 2018, n. 51 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro

processing carried out by EU institutions, bodies, offices and agencies[397]. Article 27 of Regulation 2018/1745 follows Article 25 GDPR entirely[398]. Moreover, according to the same Regulation, the processing of operational personal data in the area of freedom, security and justice applies the same DPbD rule[399].

In addition, Council Regulation 2017/1939 contains an article dedicated to DPbD. This Regulation implements enhanced cooperation on the establishment of the European Public Prosecutor's Office. The text of Article 67 is identical to the formulation of Article 25. Therefore, the office of EU Public Prosecutor shall implement appropriate technical and organisational measures designed to be compliant with the data protection principles and requirements by design[400].

Furthermore, in accordance with Regulation 2018/1240 establishing a European Travel Information and Authorisation System, the development of the EU central system shall follow the principle of data protection by design[401]. The need to build products, services, and processes in a

---

2008/977/GAI del Consiglio. 18G00080. G.U. Serie Generale n. 119 del 24–05–2018.

397 *See* Article 1(1), Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. PE/31/2018/REV/1. O.J. L. 295, 21.11.2018.

398 Article 27 Regulation (EU) 2018/1725.

399 *See* Article 85 Regulation (EU) 2018/1725.

400 Article 67(1), Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'). O.J. L. 283, 31.10.2017. *See* Hans-Holger Herrnfeld. "Article 67 Data protection by design and by default". In: *European Public Prosecutor's Office*. Nomos, 2021, pp. 513–514. ISBN: 9783848748846.

401 Article 73(3), Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226. PE/21/2018/REV/1, O.J. L. 236, 19.9.2018: "(...) The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination. In this regard, the tasks of eu-LISA shall also be to: (a) perform a security risk assessment; (b) follow the principles of privacy by design and by default during the entire lifecycle of the development of ETIAS; and (c) conduct a security risk assessment regarding the interoperability of ETIAS with the EU information systems and Europol data referred to in Article 11".

way that follows the principles of security-by-design and privacy-by-design is stressed by the Cybersecurity Act[402]. This Regulation defines the objectives, tasks and organisational matters for ENISA and creates the framework for establishing and coordinating European cybersecurity certification schemes[403].

Finally, a provision of DPbD is expected in the future e-Privacy Regulation for cookies[404]. It is worth noting that the GDPR does not apply to processing of electronic communications services in public communication networks under Directive 2002/58/EC because this legislation is a *lex specialis*[405]. Therefore, if there is no obligation in the future regulation, Article 25 will not be applicable in this context[406].

All of these other provisions on DPbD have been established in order to create consistency within the EU legal system, where the GDPR is the main data protection law, and to modernise the framework[407].

---

402 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). PE/86/2018/REV/1. O.J. L. 151, 7.6.2019. In particular, *see* Recitals 12 and 41.

403 *See* Article 1, Regulation 2019/881.

404 *See* Recital 23 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD). This Recital states: "the principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies' (...)". This text refers mostly to the default settings. However, the process for approval is pending and the act still in force is Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. L. 201, 31.7.2002. On the e-privacy proposal *see* Elena Gil Gonzalez, Paul De Hert, and Vagelis Papakonstantinou. "The proposed ePrivacy Regulation: the Commission's drafts and the Parliament's drafts at a crossroads?" In: *Data Protection and Privacy. Data Protection and Democracy*. Hart Publishers, 2020, pp. 267–298. ISBN: 9781509932740.

405 *See* Article 95 GDPR on relationship with Directive 2002/58/EC.

406 Bincoletto, *La privacy by design. Un'analisi comparata nell'era digitale*, p. 169.

407 Bincoletto, *op. cit.*, pp. 172–173.

As previously mentioned, Article 25 GDPR contains an enforceable obligation. The GDPR sets a deterrence model providing administrative fines in case of infringement. It is possible, therefore, that a violation of this requirement is sanctioned[408]. In detail, a supervisory authority may impose fines pursuant to Article 82 and 83 GDPR[409]. According to paragraph 2(d) of Article 83, when deciding whether to impose an administrative fine and its amount, the DPA should take into account various criteria, including "the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25" (and 32)[410]. Moreover, an infringement of the obligation of DPbD could be sanctioned with a fine of up to 10 million euro, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the previous financial year, whichever is higher[411]. In 2018, the EDPS committed to supporting coordinated and effective enforcement of Article 25 in cooperation with the EDPB[412].

Apart from the risk of incurring in sanctions, there are no incentives for design per se[413]. However, the administrative fines could be very high for controllers, especially in the case of SMEs.

The concept of DPbD in the GDPR is based on the assumption that "the conditions for data processing are fundamentally being set by the software and hardware" used for the operations[414]. In order to understand how to

---

408 As an example, in 2020 the Italian DPA fined Vodafone Italia S.p.A. 12,251,601 euro for non-compliance with general data protection principles and some requirements of the GDPR, including Article 25. In particular, the company did not implement appropriate measures and mechanisms to control data processing operations and ensure the continuous compliance of the telemarketing activities carried out during the collection of personal data. *See* further on this decision Giorgia Bincoletto. "Italy – Italian DPA Against Vodafone: History of a € 12 million Fine". In: *Eur. Data Prot. L. Rev.* 6 (4 2020), pp. 554–559; and Chapter 6, Section 6.5.

409 *See* also Chapter 6, Section 6.5.

410 Article 83(2)(d) GDPR.

411 Article 83(4)(a) GDPR.

412 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 22. Additionally, the authority committed to providing guidance on the appropriate implementation of the principle.

413 *See* the criticism in Bygrave, "Hardwiring privacy", p. 771. On the enforcement of the proposal *see* Paul De Hert. "The EU data protection reform and the (forgotten) use of criminal sanctions". In: *International Data Privacy Law* 4.4 (2014), pp. 262–268.

414 *See* Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 62.

apply and comply with this complex norm, it is necessary to investigate each part of the text in detail. For the explanation and investigation of the provision, the rule of the five *W-h* questions will be applied. The following subsection 2.4.1 provides the answer to the question "who?" identifying the subjects of the norm, while subsections from 2.4.2 to 2.4.6 deal with the complexity of the "what?". The answers to "when?" and "where?" are expressed in subsection 2.4.7. The remaining subsection 2.4.8 addresses the rationales and the "why?". In the end, the data protection by default requirement will be introduced in order to complete the investigation of Article 25 in section 2.4.9.

### 2.4.1 Identifying the subjects

Since Article 25 contains a legal and fully enforceable obligation, it is necessary to investigate whom shall comply with this rule. Following the GDPR definitions and requirements, the subjects involved are identified as follows.

Firstly, Article 25 explicitly refers solely to the controller. The term "data controller" refers to a "natural or legal person, public authority, agency or other body" which determines the purposes and means of the data processing[415]. This processing identifies "any operation or set of operations" that is performed on personal data[416]. When determining the purposes and means, the controller can act alone or jointly with others. If there are joint controllers, they will determine their respective responsibilities in a transparent manner through an arrangement, unless the law prescribes the conditions for them[417]. Moreover, the GDPR specifies that where the purposes and means of the data processing are determined by the EU or a Member State, the controller, or the specific criteria for its nomination,

415 *See* the definition in Article 4(7) GDPR. On the complexity of defining the data controller in practice and of distinguishing this subject from the processor, *see* Alessandro Mantelero. "Gli autori del trattamento dati: titolare e responsabile". In: *Giurispudenza Italiana* 171.12 (2019), pp. 2799–2805.

416 *See* the definition in Article 4(2) GDPR: "processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

417 *See* Article 26 GDPR.

may be provided for by Union or Member State law[418]. Each controller is fully liable for the processing under joint controllership[419].

It is worth mentioning the material and territorial scopes of the GDPR in order to restrict the data controllers that shall adopt DPbD rule.

According to the material scope of the GDPR, this regulation does not apply to data processing in the course of an activity which falls outside the scope of EU law (e.g. Member States' national security)[420]. Member States' activities on border checks, asylum and immigration are out of the scope of the regulation, too[421]. If a natural person processes data in the course of a purely personal or household activity, he or she is not considered a data controller subjected to the GDPR[422]. As noted above, Directive 2016/680 and its national implementations apply for law enforcement purposes. Finally, as previously mentioned, for data processing carried out by EU institution, bodies, offices and agencies, Regulation 2018/1745 applies. Since this Regulation contains an equal requirement, all the analysis of Article 25 is still pertinent for this material scope and the authorities, agencies and bodies included.

As regards the territorial scope, the GDPR applies to "the processing of personal data in the context of the activities of an establishment of a controller in the EU", regardless of whether the processing takes place there[423]. If the controller is not established in the EU, but the personal

418 *See* Article 4(7) GDPR.

419 *See* Article 82(4) GDPR.

420 *See* Article 2(a) GDPR. In order to understand the scope, it is necessary to read the Treaty on European Union and the Treaty on the Functioning of the European Union. *See* the Consolidated version, Official Journal C. 326, 26/10/2012, p. 1–390. There are no substantial differences with the Data Protection Directive.

421 *See* Article 2(b) GDPR.

422 *See* Article 2(c) GDPR. This rule represents the so-called "house-holder" exception.

423 *See* Article 3(1) GDPR. *See* Dan, Jerker B. Svantesson. "Chapter I General Provisions (Articles 1–4). Article 3. Territorial scope". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 74–99. ISBN: 9780198826491; Christopher, Kuner. *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*. University of Cambridge Faculty of Law Research Paper No. 20/2021. On the notion of establishment *see* the Court of Justice case law. In particular, *see* the cases C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, which ruled: "Article 4(1)(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement

data relate to data subjects who are in the EU, the GDPR applies when the processing activities are related either to the offering of goods or services or to the monitoring of individuals' behaviour (e.g. targeting or profiling), as far as their actions takes place within the EU[424]. The last scenario where the GDPR applies is the processing carried out by a controller who is not established in the EU, but in a place where a Member State's law applies by virtue of public international law[425].

Data controllers that process personal data in accordance with the material and territorial scopes of the GDPR shall comply with the DPbD obligation and are accountable and liable for it. Despite the explicit text of Article 25, the data controller is not the only subject that has to be mentioned here. Another role that is central for data processing is the processor.

According to the GDPR's definitions, the processor is "a natural or legal person, public authority, agency or other body" which processes personal

---

of such data must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity – even a minimal one – in the context of which that processing is carried out. In order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned"; and C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*, which ruled: "Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State". *See* also EDPB European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*. European Data Protection Board, 2019.

424 *See* Article 3(2)(a) – (b) GDPR.

425 *See* Article 3(2)(a) – b) GDPR.

data "on behalf of the controller"[426]. The GDPR imposes constraints on the role of the processor. Data controllers must use trustworthy processors that provide sufficient guarantees to meet the requirement of the GDPR[427]. Therefore, processors (e.g. sub-contractors or service providers) shall implement appropriate technical and organisational measures in order to ensure that the controller complies with Article 25. Moreover, processors shall implement appropriate technical and organisational measures for securing processing in accordance with Article 32 GDPR[428].

A contract between controller and processor will govern the processing delegated by the former to the latter[429]. Even though the DPbD requirement does not refer to processors, they have to collaborate with the controllers and assist them in fulfilling the DPbD obligation in a transparent manner. The contract can take into account DPbD in one or more clauses so as to ensure that the processor considers the state of the art, the cost of implementation and the characteristics of the delegated processing, and to show that the measures have been implemented. Contractual liability protects the controller. Nonetheless, the controller will remain liable for violation of the legal requirement[430]. Despite calls to extend the obligation during the legislative process, it pertains only to data controller[431].

As regards the recipient and the third party, it seems that when they have access to personal data they do not have to fulfil the GDPR's obligation because they do not define the conditions of the processing[432].

---

426 *See* Article 4(8) GDPR.

427 Indeed, Article 28(1) GDPR states: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject".

428 *See* Article 28(3)(c) and (f) GDPR.

429 Article 28(3) GDPR reads as follows: "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller (...)".

430 On liability issues *see* further Chapter 6, Section 6.5.

431 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 173.

432 *See* the definition of these subjects in Article 4(9) and (10) GDPR. The recipient is any person to whom personal data is disclosed, whether a third party or not. This last subject is a person other than the other subjects who is authorised to process personal data under the direct authority of the controller or processor.

Developers, programmers and engineers are not included in the legal provision. The disconnection between controllers and engineers questions the efficiency of the DPbD implementation strategy[433]. The EDPS wrote that the missed reference to developers is a serious limitation of the obligation[434].

Despite this obvious consideration, Recital 78 of the GDPR is a good tool for the interpreter because it connects Article 25 with the concept of accountability, expanding the concept of DPbD in the GDPR[435]. Recitals do not impose a legal obligation. However, Recital 78 explicitly refers to developers:

> "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations".

Producers of products, services and applications do not have a direct obligation under GDPR, but they could help controllers comply with DPbD requirements[436]. So, during the development and design process developers are encouraged to keep DPbD in mind, especially as data minimisation[437]. Developers should consider the application of DPbD because "data

433 *See* the comment on the EU strategy in Bygrave, "Hardwiring privacy", p. 771.

434 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 8.

435 *See* e.g. Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*, p. 29; Sartore, "Privacy-by-design, l'introduzione del principio nel corpus del GDPR", p. 301.

436 *See* Marit Hansen et al. *Recommendations on shaping technology according to GDPR provision. Exploring the notion of data protection by default*. European Union Agency for Network and Information Security, 2018, p. 5; Simone Calzolaio. "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679". In: *Federalismi.it* 24 (2017), pp. 1–21. Bygrave argued that the encouragement set by Recital 78 is a "less stringent requirement". *See* Bygrave, "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default", p. 578.

437 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 62.

controllers might select products and services on the basis of the adopted design choices"[438]. Thus, the market might be shaped in a "privacy-friendly direction"[439].

In November 2019 the European Data Protection Board released "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" to provide further guidance on that specific obligation prescribed by the GDPR[440]. After public consultation, the EDPB adopted the final version of the Guidelines on 20 October 2020[441]. These Guidelines are addressed to data controllers, but "processors and producers" are indicated as potential addressees and "key enablers" for data protection by design and by default[442]. According to the authority, producers can cooperate with the controller to achieve the implementation of the measures since design choices are inevitably influenced by developers and their expertise[443]. As a result, they can obtain a competitive advantage in the market[444].

438 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 169.

439 Bygrave, "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default", p. 578.

440 EDPB European Data Protection Board. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. 13 November 2019. Version for public consultation. European Data Protection Board, 2019.

441 EDPB European Data Protection Board. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. 20 October 2020. Version 2.0. European Data Protection Board, 2020. On this version *see* the report Giorgia Bincoletto. "European Union – EDPB Guidelines 4/2019 on Data Protection by Design and by Default". In: *Eur. Data Prot. L. Rev.* 6 (4 2020), pp. 574–579.

442 As regards this aspect of the EDPB's Guidelines 4/2019 version 1, the authority stated that "other actors, such as processors and technology providers, who are not directly addressed in Article 25, may also find these Guidelines useful in creating GDPR-compliant products and services that enable controllers to fulfil their data protection obligations". In the second version, the EDPB specified that: "The EDPB provides recommendations on how controllers, processors and producers can cooperate to achieve DPbDD. It encourages the controllers in industry, processors, and producers to use DPbDD as a means to achieve a competitive advantage when marketing their products towards controllers and data subjects".

443 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, points 1, 94, 95 and 96. *See* also Bincoletto, "European Union – EDPB Guidelines 4/2019 on Data Protection by Design and by Default", p. 575.

444 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, point 9.

The EDPB provided a step-by-step guidance for data controllers to comply with Article 25 GDPR. The authority interpreted the requirements of DPbD and DPbDf, investigated how data protection principles and rights could be implemented effectively, and listed key design and default elements with several concrete examples on data processing operations[445]. With this guidance, the text of Article 25 seems less vague than before. However, the EDPB included few notes on appropriate engineering methodologies or suitable technical approaches. In fact, despite the encouragement for processors and producers on cooperating for the implementation of Article 25, it can be argued that the language and the meaning of the document are more understandable by legal experts than by other practitioners[446].

The EDPB defines the core obligation of Article 25 as "the implementation of appropriate measures and necessary safeguards that provide effective implementation of the data protection principles and, consequentially, data subjects' rights and freedoms by design and by default"[447]. In order to effectively implement principles and rights, technical and organisational measures shall be implemented. In the next subsections the core of the provision will be analysed starting from the measures.

### 2.4.2 Defining technical and organisational measures

As noted above, the Data protection Directive already called for the implementation of measures[448]. The wording "technical and organisational measures" appears 18 times in the GDPR, in Chapter IV on controller and processor especially.

---

445 Bincoletto, "European Union – EDPB Guidelines 4/2019 on Data Protection by Design and by Default", p. 575.

446 Bincoletto, *op. cit.*, p. 579.

447 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 4. In the first version of the Guidelines the EDPB defined the core obligation as "the effective implementation of the data protection principles and data subjects' rights and freedoms by design and by default". *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.

448 Recital 46, Article 17 Directive 95/46/EC. *See* Article 29 Working Party, Police, and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, p. 13.

According to Recital 78 GDPR, these measures are necessary for the protection of the rights and freedoms of natural persons with regard to the processing of personal data in order to ensure that the requirements of the GDPR are met[449]. The measures of DPbD are a sub-category of all the measures that the controller shall implement, and they particularly aim to demonstrate compliance with the Regulation[450].

The Recital mentioned above specifies that such measures could consist in[451]:

> "minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features".

Therefore, the list of the possible measures is technologically neutral and open. The same strategy is used in the text of Article 25, where the "appropriate technical and organisational measures" are undefined. Commentators point out that the list remains very high-level and fails to give guidance[452].

As a matter of fact, the term "measure" should be understood broadly as any method or means that can be employed[453]. Actually, the legal requirement does not define a specific level of sophistication but indicates that the measures shall be appropriate for implementing data protection principles effectively[454]. Adopted and implemented measures should be documented and described in detail. It is not an explicit requirement.

449 Recital 78 GDPR.
450 *Ibid.*
451 *Ibid.*
452 *See* Rubinstein and Good, "The trouble with Article 25 (and how to fix it): the future of data protection by design and default", pp. 5–6.
453 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, point 8.
454 *See* European Data Protection Board, *op. cit.*, point 9. According to the authority, "examples that may be suitable, depending on the context and risks associated with the processing in question" include: "pseudonymization of personal data; storing personal data available in a structured, commonly machine readable format; enabling data subjects to intervene in the processing; providing information about the storage of personal data; having malware detection systems; training employees about basic "cyber hygiene"; establishing privacy and information security management systems, obligating processors contractually to implement specific data minimisation practices".

Nonetheless, in order to demonstrate compliance with the accountability principle the controller shall support the implementation with documents and reports.

Measures can be organisational or technical. These two categories and levels connect DPbD with the typical global PbD approach, which usually requires both policy strategies and technical solutions. Organisational measures are focused on policy and management levels, while technical measures are the manifestation of a technical design. It is worth mentioning that PETs, as specific technical solutions, can be used for assisting the DPbD implementation.

The explicit mention in Article 25 identifies pseudonymisation as an appropriate measure. However, it should be pointed out that the data controller always has to take into account all the various criteria expressed in the first part of the provision. If there is no need, pseudonymisation is not necessary. As mentioned, Recital 78 proposes minimisation, measures to enhance transparency and control, and measures to create and improve security during processing.

The example of pseudonymisation suggests a starting point for implementation that was not present in the draft of the Regulation. This specification does not preclude any other measure[455]. Pseudonymisation may just be a core strategy for DPbD[456]. It should be promoted as a DPbD measure by the authorities[457]. The GDPR uses this term to identify the processing of personal data where the personal data can "no longer be attributed to a specific data subject without the use of additional information", which is "kept separately" and is subject to technical and organisational measures in order to ensure that the personal data are not attributed to an identified or identifiable natural person[458]. So, pseudonymisation is strictly related to the identifiers of natural persons and pseudonymised data is still personal data. The identifier is the identifying information of

455 *See* Recital 28 GDPR.

456 *See* ENISA European Union Agency for Network & Information Security. *Recommendations on shaping technology according to GDPR provision. An overview on data pseudonymisation*. European Union Agency for Network and Information Security, 2018, p. 4.

457 *See ibid.* According to the agency, DPAs and EDPB should promote the strategy and provide guidance for controllers.

458 Article 4(5) GDPR. *See* also Luca Tosoni. "Chapter I General principles (Articles 1–4). Article 4(5). Pseudonymisation". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 132–137. ISBN: 9780198826491.

the data subject. It can be a single piece of information or more complex data. The pseudonym is the information that substitutes that identifier after the pseudonymisation process. The additional information refers to the association between the mentioned identifier and the pseudonym. With the additional information, the pseudonym can be re-identified[459]. Pseudonymisation focuses on hiding the identifier[460].

ENISA defined pseudonymisation as follows[461]:

> "In broad terms, pseudonymisation refers to the process of de-associating a data subject's identity from the personal data being processed for that data subject. Typically, such a process may be performed by replacing one or more personal identifiers, i.e. pieces of information that can allow identification (such as e.g. name, email address, social security number, etc.), relating to a data subject with the so-called pseudonyms, such as a randomly generated values".

According to the Agency, the definition of the GDPR goes beyond a purely technical definition. In particular, the GDPR covers the protection of indirect identifiers relating to a data subject and additional information, too[462]. The main benefit of using pseudonymisation is hiding the identity of the data subject to any third party[463]. Moreover, if the data controller does not need the identifier for the processing, this subject can process only pseudonymised data, ensuring data protection by design[464]. The result of the application of this measure is the reduction of data-protection risks[465]. Indeed, pseudonymisation technically reduces the level of this risk[466].

---

459 For this explanation, *see* European Union Agency for Network & Information Security, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation*, p. 9.

460 *See* European Union Agency for Network & Information Security, *op. cit.*, p. 17. By contrast, encryption ensures that the whole dataset of identifiers is unintelligible.

461 *See* European Union Agency for Network & Information Security, *op. cit.*, p. 9.

462 *See ibid.*

463 *See* European Union Agency for Network & Information Security, *op. cit.*, p. 15.

464 *See ibid.*

465 *See* Recital 28 GDPR.

466 As regards the techniques for pseudonymisation and DPbD, *see* ENISA European Union Agency for Network & Information Security. *Recommendations on shaping technology according to GDPR provisions. Pseudonymisation techniques and best practices*. European Union Agency for Network and Information Security, 2019; Giuseppe D'Acquisto and Maurizio Naldi. *Big data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*. Torino: G. Giappichelli Editore, 2017. ISBN: 9788892106291, pp. 37–40. 117; another study that connects the

The next subsections investigate the established text on conditions of Article 25 that have to be taken into account when selecting and implementing technical and organisational measures. Balancing all the criteria is challenging. Therefore, the following subsections will provide some guidance on defining the criteria and explaining how they relate to one another.

### 2.4.3 Understanding the state of the art and balancing the costs of implementation

Article 25 defines the criteria that have to be balanced in applying the legal requirement. The first condition is the state of the art, while the second is the cost of implementation.

The expression *state of the art* is used in Article 25 and 32 of the GDPR[467]. However, the Regulation does not provide a definition of this criterion. In the legal domain the state of the art is frequently used in product liability and safety rules, environmental protection and IP and patent law, and their respective case law[468].

---

two concepts is D'Acquisto et al., *Intelligenza artificiale, protezione dei dati personali e regolazione*, pp. 116–119. Anonymisation guarantees more protection, but it is not always feasible, and scholars have proven that de-anonymisation is a concrete and high risk. The GDPR does not concern anonymous data in accordance with Recital 26. However, anonymised data differs from anonymous data because the former is personal data that has been anonymised after a process, while the latter is data that cannot be attributed to a natural person theoretically. Before the process of anonymisation, and until the end, the GDPR applies. On anonymisation techniques, *see* WP29 Article 29 Working Party. *Opinion 05/2014 on Anonymisation Techniques*. WP216 14/en, 2014. The Opinion refers to Directive 95/46/CE, but its general considerations are still applicable. *See* also Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, pp. 123–130; Stefano Torregiani. "Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, *ownership* e *Data by Design*". In: *Federalismi.it* 18 (2020), pp. 317–341, pp. 322–326.

467 *See* also Recitals 78 and 83.

468 As an example, *see* some Court of Justice case law at <curia.europa.eu>: Case C-121/17 Teva UK and Case C-190/16 Werner Fries. In particular, in the Opinion of the Advocate General on case C-190/16 highlightes that the state of the art includes the "best practices, and scientific and technical progress in the field of (...)". In the legal domain the expression does not always have the same meaning. As regards patent law, according to paragraph 1 of Article 54 of the European Patent Convention "an invention shall be considered to be new if it

The first criterion is objective and dynamic. It refers to the existing scientific knowledge in a specific field. The state of the art includes both organisational and technical solutions.

In 2020 the German association TeleTrusT released the Guidelines "State of the Art" on IT security in cooperation with ENISA[469]. These Guidelines mention both Article 25 and 32 of the GDPR. This document specifies that the definition of state of the art shall be distinguished from the "generally accepted rules of technology" and the "existing scientific knowledge and research". The distinction is borrowed from the German case law[470]. In the middle of these two criteria there is the state of the art which can be described as "the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives"[471]. A practical evaluation method can concretely determine the state of the art[472]. It can be suggested that this definition is useful for understanding what the state of the art in Article 25 is. Indeed, the EDPB quoted this approach in the Guidelines on DPbD[473].

In sum, the state of the art criterion requires taking into account what is currently available in the market for technical and organisational measures in order to achieve the effective implementation of the data protection principles. Data controllers should stay up to date on technological progress; and standards, codes of conduct and certification mechanisms could indicate the state of the art within a specific field[474]. To be com-

---

does not form part of the state of the art". The expression here refers to what generally exists earlier, including filed applications.

469 *See* TeleTrusT IT Security Association Germany. *Guidelines "State of the Art"*. TeleTrusT and ENISA, 2020.

470 TeleTrusT reported that the distinction follows the Federal Constitutional Court's Kalkar decision of 1978 (BVerfGE, 49, 89 – 135 f).

471 IT Security Association Germany, *Guidelines "State of the Art"*, p. 11. The short definition is: "a subject's best performance available on the market to achieve an object", where the "subject is the IT security measure" and "the object is the statutory IT security objective".

472 *See* IT Security Association Germany, *op. cit.*, p. 12. The mentioned Guidelines described the method for evaluating the state of the art. This method is based on average scores of two conditions. The x-axis shows the degree of proof in practice, while the y-axis shows the degree of recognition. They should both be measurable.

473 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 8.

474 European Data Protection Board, *op. cit.*, 8, point 19.

pliant with this dynamic requirement, the criterion should be evaluated continuously on the basis of technological advancements[475].

Secondly, the controller shall take into account the cost of implementation while estimating the alternative measures. Therefore, the cost of the measures existing in the state of the art is a subjective criterion. This criterion has been defined as economic feasibility: the legal requirement does not mandate unreasonably costly measures to the data controller[476]. So, the cost of DPbD should be feasible for the controller. The data controller can choose the measures available in the market at a reasonable price[477].

In general, costs are all the expenses that the controller has to bear from planning to implementation. It is arguable that these expenses are appropriate if suited to the level of protection required[478]. Therefore, during the selection of the measures what matters is if they adequately protect personal data. In the market there are several proprietary tools and solutions for protecting personal data. The costs are set by the private entities that have developed these tools. It is possible that unreasonably high costs are set. As a result, some controllers probably cannot afford such expense.

The EDPB explained that time, business costs and human resources should be taken into account when planning the cost of implementation. Cost is more than money[479]. Article 25 refers to the cost of implementing data protection principles during processing. Data controllers should plan and pay the costs that are necessary for this implementation[480]. The authority specified that inability to bear the costs does not excuse liability, but effective implementation must not necessarily lead to higher costs[481].

Both criteria are fundamental for planning DPbD measures. The condition of the state of the art encourages the controller to stay up-to-date, but the cost criterion allows a cost-benefit analysis for estimating the alternatives.

---

475 European Data Protection Board, *op. cit.*, 8, point 20. *See* also Bincoletto, "European Union – EDPB Guidelines 4/2019 on Data Protection by Design and by Default", p. 577.

476 Hildebrandt and Tielemans, "Data protection by design and technology neutral law", p. 517.

477 *See* Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 184.

478 *See* Tamó-Larrieux, *op. cit.*

479 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 9, point 23.

480 European Data Protection Board, *op. cit.*, p. 9.

481 *Ibid.*

Another important and explicit criterion of Article 25 that tailors the measures to the controller are the specifics of processing, i.e., its nature, scope, context and purposes. It will be analysed in the following subsection.

### 2.4.4 Evaluating the nature, scope, context and purposes of data processing

Article 25 requires evaluating and taking into account the "nature, scope, context and purposes" of processing. These contextual factors represent the characteristics of data processing operations[482]. They are subjective conditions. According to Bygrave, these factors may be largely determined by the controller during the DPIA[483].

Firstly, nature is actually the inherent characteristics of the processing[484]. It can be argued that the nature is the type of activity or operation of which the processing consists (e.g. collection, storage, disclosure)[485]. Moreover, the nature relates to the way the processing is carried out (e.g. automated means)[486]. Different operations need different safeguards. As an example, the controller should implement specific technical and organisational measures during the disclosure by transmission and others for the storage of personal data.

---

482 European Data Protection Board, *op. cit.*, 9, point 28.

483 Bygrave, "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default", p. 576.

484 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 9, point 28.

485 On the possible activities, *see* the open list in Article 4(2) GDPR reported *supra* note no.416.

486 *See* the interesting questions that the controller can raise in Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 179: "what means are used for the processing operation (e.g., automated)? Is the processing going to result in profiling of individuals that will allow evaluating the personal aspects relating to an individual whose data are being processed? Are there any third parties that are included in the processing? Is the processing carried out by a cloud-based infrastructure? Does the processing include aggregation of data sets? Is the processing activity performed outside the EU?".

Secondly, the scope of processing relates to its size and range[487]. Generally, the GDPR gives importance to the size and scale of processing[488]. The controller should choose the measures taking into account the range of personal data being handled, meaning how many data subjects are there and who are they, and which types of data are involved[489].

Thirdly, context refers to the circumstances of processing[490]. With this criterion the controller takes into account where processing takes place. This is also a metaphorical setting. The word refers to the situation and set of circumstances that constitute processing.

Lastly, purpose is one of the main concepts of data protection law. It refers to the aim of the processing operation[491]. According to Article 5(19)(b) GDPR, the purpose should be specified, explicit, legitimate and limited. When planning DPbD the purpose of each operation or set of operations shall be carefully considered.

In a report on security of processing ENISA identified seven questions that help companies define their processing operations and their contexts[492]. These questions represent the minimum to be asked for each processing operation and may be useful for DPbD planning. They are listed as follows:

- What is the personal data processing operation?
- What are the types of personal data processed?
- What is the purpose of the processing?
- What are the means used for the processing of personal data?[493]
- Where does the processing of personal data take place?

---

487 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 9, point 28.

488 *See* Article 30(5) GDPR on the record and Article 35(3) GDPR on DPIA.

489 As will be explained in the following Chapters, personal health data should be processed with stronger safeguards.

490 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 9, point 28, which mentioned that the circumstances may influence the expectations of the data subject.

491 European Data Protection Board, *op. cit.*, 9, point 28.

492 *See* D'Acquisto and Panagopoulou, *Guidelines for SMEs on the security of personal data processing*, pp. 18–19. The same questions are reported in another report on security of personal data processing. *See* ENISA European Union Agency for Network & Information Security. *Handbook on Security of Personal Data Processing*. European Union Agency for Network and Information Security, 2017, p. 10.

493 As an example, the means could be automated or not.

– What are the categories of data subjects?[494]
– What are the recipients of the data?

After the state of the art, the cost of implementation and the characteristics of the processing, the last element to be taken into account is a specific risk analysis. Next subsection investigates this factor of Article 25.

### 2.4.5 Evaluating the risks posed by data processing

Generally, the GDPR requires taking into account a risk assessment. Risks are possible scenarios describing events and their consequences that are estimated in terms of severity and likelihood[495]. Risk management refers to the "coordinated activity to direct and control an organisation with regard to risk"[496].

After the GDPR, risk management has become a substantial part of corporate management activities. From an historical point of view, the concept of risk exists since the beginning of informational privacy and data protection law[497]. As will be explained in the following section on related requirements, the risk management approach has been further specified in Article 35 of the GDPR dedicated to the Data Protection Impact Assessment (hereinafter: DPIA).

Article 25 always requires taking into account any "risks of varying likelihood and severity for rights and freedom posed by the processing". Risks are criteria for determining the concrete measures to be implemented. Risk management is at the core of DPbD[498]. The approach is dynamic, and

494 Usually law prescribes particular rules for the processing of personal data related to children. The GDPR sets Article 8 for defining the conditions applicable to child's consent in relation to the offer of information society services.

495 WP29 Article 29 Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. WP248 17/en, 2017, p. 6.

496 *Ibid.*

497 *See* Alessandro Mantelero. "Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32–39)". In: *Il nuovo Regolamento europeo sulla privacy e protezione dei dati personali*. Zanichelli, Torino, 2017, pp. 287–330. ISBN: 9788808521057, p. 294; Alessandro Mantelero. "La gestione del rischio". In: *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*. Zanichelli, Torino, 2019, pp. 449–502. ISBN: 9788808820433, p. 452.

498 European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 8.

enables the identification and integration of the measures according to the concrete risks for individuals. Therefore, the measures are not the same under all operations. Once again, a "one-size-fits-all" approach does not comply with the legal requirement. The recommendation in the EDPB's Guidelines on Article 25 was to "always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed", independently of the application of Article 35 GDPR[499].

The term "severity" indicates the magnitude of a risk, whereas "likelihood" expresses the possibility of a risk occurring[500]. The scale of severity could define the levels as low, medium, high and very high in relation to the consequences that the situation has on individuals. The evaluation of severity for right and freedoms is qualitative[501]. To assess the likelihood of risks, the evaluation is performed through probability rules and the levels could be estimated as negligible, limited, significant and maximum, all of which have different scores. To identify the risk as a whole, the controller should multiply the likelihood value by the impact value[502].

As regards the wording "rights and freedoms of natural persons", it should be pointed out that the GDPR frequently refers to fundamental rights and freedoms recognised in the Charter of Fundamental Rights of the European Union. In particular, the Regulation honours the right to respect for private and family life, home and communications (Art. 7), the protection of personal data (Art. 8), freedom of thought, conscience and religion (Art. 10), freedom of expression and information (Art. 11), freedom to conduct a business (Art. 16), the right to an effective remedy and to a fair trial (Art. 47), and cultural, religious and linguistic diversity (Art. 22)[503]. Other rights and freedoms are recognised by the same Charter. Therefore, the data controller shall assess the possible risks in relation to these rights and freedoms, and the subject shall evaluate their severity

499 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.

500 CNIL Commission Nationale de l'Informatique et des Libertés. *Privacy Impact Assessment (PIA). Method- ology*. 2018, p. 6. For more details on the CNIL's approach, *see* Chapter 5, Section 5.4.

501 On this regard, *see* e.g. D'Acquisto and Panagopoulou, *Guidelines for SMEs on the security of personal data processing*, p. 20.

502 All the technical aspects on risk assessment will be presented in Chapter 5, Section 5.4.

503 *See* Recital 4 GDPR. On these rights and data protection law *see* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*.

and likelihood and then select the DPbD measures accordingly and proportionally[504].

### 2.4.6 Defining "appropriate" and "effective" criteria

Article 25 specifies that the measures shall be *appropriate* because they are designed to implement data protection principles in an *effective* manner. According to the EDPS, the two adjectives represent a special dimension of the DPbD obligation[505]. Effectiveness is at the heart of the concept of DPbD[506].

Firstly, it has been argued that "appropriate" entails a free discretion of the data controller[507]. This adjective implies the contextual and dynamic nature of the legal provision[508]. However, this discretion could always be scrutinised by the DPA or by a court. Measures are appropriate when they are designed to implement data protection principles (Art. 5 GDPR). As mentioned above, pseudonymisation has been explicitly indicated as appropriate.

Secondly, implementation shall be performed "in an effective manner". It is clear from the text that the goal is again the implementation of data protection principles. In order to address effectiveness, specific and dedicated measures shall be implemented for each processing operation and principle[509]. Generic measures are not sufficient nor effective. Chosen measures must be specific to the particular processing and robust[510].

Effectiveness relates to the proportionality principle which is used in the risk management approach[511]. As a result, this criterion can be a contextu-

504 On the risk management approach *see* also Section 2.5.2.
505 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 6.
506 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 7, point 13.
507 *See* Hildebrandt and Tielemans, "Data protection by design and technology neutral law", p. 517.
508 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 173.
509 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.
510 *See* European Data Protection Board, *op. cit.*, 7, point 14.
511 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 176.

al and measurable parameter that requires a professional judgement by experts[512].

It should be noted that Article 25 also requires the integration of necessary safeguards into the processing in order to meet the requirements of the GDPR and protect data subjects' rights. This expression follows the effective criteria but seeks consideration of all the provisions of the regulation. Appropriate measures shall be designed to integrate such safeguards.

The EDPB pointed out that "whether or not measures are DPbDD-compliant" depends on the "contexts of the particular processing in question and an assessment of the elements that must be taken into account when determining the means of processing"[513]. In order to demonstrate compliance and effectiveness (i.e. the measures are appropriate in an effective manner and safeguards are integrated), the controller can define and use subjective or objective metrics and "key performance indicators" (KPI), meaning measurable values that can demonstrate "how effectively the controller achieves their data protection objective"[514]. Alternatively, the subject may provide the rationale behind the chosen measures and safeguards.

However, there is no uniform or accredited approach in the literature. Documenting the implementation and explaining in detail the adopted solutions remain first reliable strategies. It can be argued that the vagueness and uncertainty of Article 25 come to light with the appropriate and effective conditions. Courts and DPAs will give some guidance when ruling on the future case law[515].

### 2.4.7 Identifying the time aspect of the requirement

Article 25 GDPR refers to "the time of the determination of the means for processing" and "the time of the processing itself". This phrasing refers to the design phase of the processing and its concrete operations and

512 *Ibid.*

513 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 7, point 14.

514 *See* European Data Protection Board, *op. cit.*, 7, point 16. The EDPB suggested: "KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments".

515 *See* some cases in Chapter 6, Section 6.5.

activities[516]. As a result, DPbD aims to provide safeguards for the whole project and data management life cycle[517].

Thus, the measures shall be implemented before and during the concrete operations of processing. The determination of the means refers to every detailed design element[518]. Therefore, in the time of the determination the controller has not yet defined the means to be incorporated and has the opportunity to take into account all the elements.

As noted in the critical analysis on PbD, the timing is crucial for efficiency and effectiveness. The sooner the measures are planned and implemented, the better the controller complies with DPbD. However, at the time of processing the controller shall maintain DPbD[519].

During the processing operations, the DPbD measures shall be re-evaluated regularly[520].

The purpose of DPbD is to be applied throughout the entire processing life cycle, including the life cycle of an IT system and of management practices.

So far, the study has deepened the answers to who, what, how, where and when. The next subsection deals with why and the rationales of Article 25 GDPR.

### 2.4.8 Towards the implementation of principles and rights

Article 25 establishes an obligation that seeks to:

1) "implement data-protection principles, such as data minimisation, in an effective manner";
2) "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation";
3) and "protect the rights of data subjects".

It has been argued that these objectives superimpose on one another because they all aim to comply with the data protection rules and, in partic-

516 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 5.
517 *See* European Data Protection Supervisor, *op. cit.*, p. 6.
518 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 10, point 34. The EDPB uses as examples architecture, procedures, protocols, layout and appearance.
519 *See* European Data Protection Board, *op. cit.*, 10, point 35, and 11, point 37.
520 Bincoletto, "European Union – EDPB Guidelines 4/2019 on Data Protection by Design and by Default", p. 577.

ular, with the GDPR and the principles provided[521]. The entire GDPR contains 99 provisions. The appropriate measures shall be designed to ensure compliance with the entire Regulation[522]. However, distinct attention should be paid to principles and rights. DPbD aims to build principles for improving their traction[523].

As regards data protection principles, Article 5 GDPR has been mentioned frequently[524]. This provision sets out the principles relating to all processing of personal data. Scholars have argued that Article 25 is not clear about its scope because it mentions data minimisation only[525]. Another commentator criticised Article 25 by defining it a "catch-all provision with no specific requirements of its own"[526]. These claims might be persuasive, but they should be contested by a deeper analysis of the provision that aims to advocate for its concrete application.

For the present purposes, the principles will be analysed separately as presented in the following Table 2.2. The analysis presents the principles in connection with DPbD and provides brief implementation notes[527]. Detailed guidance for implementing the principles cannot be provided because concrete implementation is sector- and case-specific[528]. Nevertheless,

521 *See* Sartore, "Privacy-by-design, l'introduzione del principio nel corpus del GDPR", p. 300. The author stressed that the mention of the principle was only added in the final version of the text.

522 Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 175.

523 Bygrave, "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default", p. 573.

524 On all the principles *see* also Recital 39. Generally on all the principles of the GDPR *see* Cuffaro, D'Orazio, and Ricciuto, *I dati personali nel diritto europeo*, pp. 179–218; Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, pp. 115–135; Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, pp. 87–92; Bolognini, Pelino, and Bistolfi, *Il regolamento privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati, in vigore da maggio 2016*, pp. 92–118.

525 *See* Rubinstein and Good, "The trouble with Article 25 (and how to fix it): the future of data protection by design and default", p. 5.

526 Waldman, "Privacy's Law of Design". In Waldman, "Data Protection by Design? A Critique of Article 25 of the GDPR", p. 153, the author once again defines Article 25 a "catch-all provision" that is "repetitive of other sections of the GDPR and has no identity of its own".

527 Chapter 3 gives more technical considerations for the healthcare context.

528 Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 167.

some organisational and technical measures to achieve each principle can be presented here[529].

*Table 2.2 Data protection principles*

| PRINCIPLE | DEFINITION |
|---|---|
| Lawfulness | Personal data shall be processed lawfully |
| Fairness | Personal data shall be processed fairly |
| Transparency | Personal data shall be processed in a transparent manner in relation to the data subject |
| Purpose limitation | Personal data shall be collected for specified, explicit and legitimate purposes |
| Data minimisation | Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes |
| Accuracy | Personal data shall be accurate and, where necessary, kept up-to-date |
| Storage limitation | Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes |
| Integrity and Confidentiality (security) | Personal data shall be processed in a manner that ensures appropriate security of the personal data |
| Accountability | The controller shall be responsible for, and be able to demonstrate compliance with, principles |

529 As mentioned, the EDPB provided a list of key and guiding DPbD and DPbDf elements for each of the principles of Article 5. *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, pp. 14–28.

The lawfulness principle essentially means that processing shall respect all applicable legal requirements[530]. In order for processing to be lawful, personal data shall be processed on a legitimate basis[531]. The legal grounds of processing are provided in Articles 6 and 9, and some specifications are set by Articles 7, 8 and 10 GDPR. For the processing of personal data, the lawful legal grounds are: a) data subject's consent; b) the performance of a contract; c) a legal obligation under Union or Member State law; d) the vital interest of the data subject or of another natural person; e) the performance of a task in the public interest set out by Union or Member State law; and f) a legitimate interest pursued by the data controller or a third party[532].

On the one hand, in order to implement the lawfulness principle at the time of the determination of the means the data controller shall define the legal basis for each processing operation or activity. On the other hand, during the processing life cycle the controller shall implement measures for ensuring that the processing operation or activity is in line with the legal basis[533]. Documents, such as consent forms and contractual clauses, should be prepared if consent or the contract is the legal ground. An assessment of the legitimate interest should be performed to understand whether such interest is overridden by interests or fundamental rights and freedoms of the data subject which require protection of personal data[534]. If and when the legal basis ceases to apply, measures should be

530 Cécile De Terwangne. "Chapter II Principles (Articles 5–11). Article 5. Principles relating to processing of personal data". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 309–397. ISBN: 9780198826491, p. 314.

531 *See* Recitals 39 – 48 GDPR.

532 As regards the legal basis for special data (Art. 9), *see* Chapter 3. Each legal basis is further specified in Article 6. Article 7 sets some conditions for consent which generally has to be freely given, specific, informed and unambiguous (Art. 4(11)). Other conditions applicable to child consent are required by Article 8. On consent *see* also WP29 Article 29 Working Party. *Guidelines on consent under Regulation 2016/679*. WP259 17/en, 2017. Article 10 specifies that processing of personal data relating to criminal convictions and offences shall be carried out only under particular controls. On the legal basis of the GDPR *see* e.g. Fabio Bravo. "Il consenso e le altre condizioni di liceità". In: *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*. Zanichelli, Torino, 2017, pp. 101–177. ISBN: 9788808521057.

533 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 16.

534 The Court of Justice elaborated the three-part test of legitimate interest under the Data Protection Directive in the case C-13/16 *Valsts policijas Rīgas regiona*

implemented to stop the processing (e.g. automatic alerts, technical configurations, internal policies). Examples are when the data subject withdraws the consent, or when the minor becomes an adult. Other grounds shall be defined.

In the GDPR the principle of fairness is always presented in connection with lawfulness and transparency[535]. Nonetheless, it represents a distinct and overarching principle of the Regulation. Indeed, the EDPB highlighted that fairness requires that "personal data shall not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject"[536]. In a fair processing personal data have not been processed through unfair means or deceptions[537]. This definition may be too vague to support the controller in a concrete implementation. However, according to the fairness principle, processing does not have unforeseeable negative effects[538]. The concept of fairness is linked to the interests and expectations of the data subject[539].

Generally, measures against discrimination, nudges and power imbalances are implementing the principle of fairness. Only taking into account the nature, scope., context and purpose of the processing is it possible to

---

*pārvaldes Kārtības policijas pārvalde contro Rīgas pašvaldības SIA "Rīgas satiksme"*. The three steps are: 1) purpose test (whether there is a legitimate interest for processing); 2) necessity test (whether the processing is necessary for the purpose); 3) balancing test (whether an individual's interests, rights or freedoms override the legitimate interest). For further discussion of this test *see* Irene Kamara and Paul De Hert. "Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach". In: *Brussels Privacy Hub* 4.12 (2018), pp. 1–35.

535 In the GDPR, as regards "lawful and fair" *see* Recitals 39 and 45, and Article 6(2) – (3). For "fair and transparent" *see* Recitals 39, 60, 71, and Articles 13(2), 14(2), 40(2).

536 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 17.

537 De Terwangne, "Chapter II Principles (Articles 5–11). Article 5. Principles relating to processing of personal data", p. 314.

538 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 117.

539 *See* Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 88.

540 In order to clarify the concept, the EDPB used several key guiding elements in the Guidelines on Article 25. Some elements are: "Autonomy – data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing; interaction – data subjects must be able to communicate and exercise their rights in respect of the personal data processed by

define some concrete examples[540]. The principle of fairness goes beyond transparency obligations and seeks an ethical processing[541].

Data subjects should be informed of the existence, extent and purposes of the processing[542]. The principle of transparency is strictly connected to providing and receiving information, and enabling data subjects to understand their rights[543]. The processing shall be transparent, meaning that it shall be clear and open for data subjects. Specific articles of the GDPR embed this principle explicitly. Article 12 defines the extent and the modalities of transparency, which is strictly connected to information and the exercise of data subjects' rights. Articles 13 and 14 list the information to provide to the data subject, whether or not the personal data is collected from the individual[544]. Lastly, Article 34 sets the conditions for the communication of a personal data breach to the data subject. These provisions describe the content of communications that the controller shall provide to the data subject, including information on privacy policies.

Therefore, organisational strategies and privacy policies should be defined to ensure transparency and easy comprehension of what the processing entails. The language shall be clear, concise and plain and the information shall be provided in a concise, intelligible and easily accessible

---

the controller; expectation – processing should correspond with data subjects' reasonable expectations; non-discrimination – the controller shall not unfairly discriminate against data subjects; non-exploitation – the controller should not exploit the needs or vulnerabilities of data subjects; consumer choice – the controller should not "lock in" their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a lock-in to the service, which may not be fair, if it impairs the data subjects' possibility to exercise their right of data portability in accordance with Article 20; respect of rights – the controller must respect the fundamental rights of data subjects and implement appropriate measures and safeguards and not impinge on those rights unless expressly justified by law". Therefore, in the authority view, fairness can be related to a data subject's rights and freedoms. Other elements suggested by the EDPB refer to ethical aspects of the data processing (e.g. human intervention and fair algorithms). Actually, fairness is a typical ethical principle.

541 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 119.

542 *See* Recital 39 and 60 GDPR.

543 *See* Article 12 GDPR. *See* also European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 15.

544 *See infra* on right to be informed.

(oral or written) form[545]. The communication of information could be targeted to the specific audience since the information should be relevant and applicable to the specific data subjects (e.g. children), and it could be layered or provided in a machine-readable form[546]. It should be noted that some information is related to technical aspects of the processing: the period of storage, the criteria for determining this period, and the existence of automated decision making with the logic that is involved[547]. As established by Article 12(2) GDPR, the exercise of the data subject's rights shall be facilitated. As a result, technical measures should be implemented in order to guarantee prompt answers to information requests, ensure the possibility of exercising the rights (e.g. by electronic means), and act upon requests referring to any right.

Moreover, the data controller can collect and process personal data only for specified, explicit and legitimate purposes. Further processing is lawful only if it is compatible with the purpose for which personal data was collected, with the exception of Article 89(1) GDPR on scientific research[548]. If the second purpose is incompatible, a new legal basis shall support the processing or personal data shall be anonymised. These statements sum-

545 For an explanation of these adjectives *see* WP29 Article 29 Working Party. *Guidelines on transparency under Regulation 2016/679*. WP260 17/en, 2018, pp. 7–10.

546 This is a key element of the EDPB's Guidelines. *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 15. Other interesting key elements of the transparency principle are: "universal design – information shall be accessible to all data subjects, include use of machine readable languages to facilitate and automate readability and clarity; comprehensible – data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups; multi-channel – information should be provided in different channels and media, not only the textual, to increase the probability for the information to effectively reach the data subject; layered – the information should be layered in a manner that resolves the tension between completeness and understanding, while accounting for data subjects' reasonable expectations".

547 *See* Article 22(1) and (4) GDPR. On the importance of transparent information about the algorithm *see* the report on an interesting case in Giorgia Bincoletto. "Italy – Supreme Court of Cassation on Automated Decision Making: Invalid Consent if an Algorithm is Not Trasparent". In Eur. Data Prot. L. Rev. 7 (2 2021), pp. 248–253.

548 The notion of "compatibile" should be interpreted on the basis of Article 6(4) of the GDPR. *See* further in De Terwangne, "Chapter II Principles (Articles 5–11). Article 5. Principles relating to processing of personal data", p. 316.

marise the rationale of the purpose limitation principle[549]. The purpose is a central concept for data protection law[550]. Any processing of personal data has a purpose. Each purpose shall be specifically defined prior to the collection of data from the very beginning[551]. A purpose shall be legitimate, and it shall not be ambiguous or kept hidden[552]. Implementing measures should limit the operations to the extent strictly necessary and proportionate to each defined purpose. Technical measures can limit the possibility of re-purposing personal data and organisational measures can control the reuse[553].

Data minimisation is the only principle explicitly mentioned in Article 25. This principle directly concerns the design of data processing systems[554]. It is connected to the principle of necessity. Measures shall ensure that personal data are adequate, relevant and limited in amount to what is necessary in relation to the purpose. As a matter of fact, data collection should be limited to what is necessary. Features and parameters of processing systems should be configured to achieve these goals, and when not possible deletion and anonymisation should occur[555]. Minimisation requires that identification of individuals should be possible only if needed for processing, meaning that pseudonymisation should be implemented, as previously explained, as well as other techniques, such as randomisation

549 *See* Article 5(1)(b), Article 6(4) and Recitals 49, 50 GDPR.

550 De Terwangne, "Chapter II Principles (Articles 5–11). Article 5. Principles relating to processing of personal data", p. 315, points out that this principle is a cornerstone of data protection law and a prerequisite for most other fundamental requirements.

551 *See* Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 90.

552 De Terwangne, "Chapter II Principles (Articles 5–11). Article 5. Principles relating to processing of personal data", p. 315. A legitimate purpose does not create disproportionate interference with data subjects' rights and freedoms on the basis of the data controller's interests.

553 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 20.

554 *See* Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 91. The author groups in the principle concerning design the principles of data minimisation, storage limitation, data security and accuracy.

555 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 21.

and generalisation[556]. Actually, the EDPB suggested avoiding the processing altogether (e.g. data avoidance, limitation) when this is possible for the relevant purpose[557].

Furthermore, personal data shall be accurate and kept up-to-date. When inaccurate, data shall be erased or rectified without undue delay[558]. Accuracy is a mathematical concept that determines how close the result of an experimental measurement can be considered to the true value of the measured quantity. In the data protection domain personal data is accurate when it is true and complete. Organisational and technical measures should decrease inaccuracy in all the phases of data processing. An accuracy policy and guidelines could be prepared at the organisational level. Accuracy should be checked regularly because potential damage might be caused to the data subject[559].

Another principle of the GDPR is storage limitation. Processing shall keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purpose. Further storage is permitted by implementing appropriate technical and organisational measures only in accordance with Article 89(1)[560]. Data controllers shall know what personal data are processed and for what amount of time they are stored for the purpose[561]. As mentioned, this information should be provided to data subjects. A retention policy and an inventory could be defined. After a certain period of time, measures should be implemented for anonymisation or erasure.

In addition, the integrity and confidentiality principles require that personal data shall be processed in a manner that ensures appropriate security. Protection against unauthorised access, unlawful processing, accidental

556 *See* e.g. Danezis et al., *Privacy and Data Protection by design – from policy to engineering*; D'Acquisto and Naldi, *Big data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*.

557 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 21.

558 *See* Article 5(1)(d) GDPR.

559 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 128. As an example, personal data related to banking information and creditworthiness shall be updated regularly in order to successfully obtain a loan from a bank.

560 *See* Article 5(1)(e) GDPR.

561 The EDPB noted that "it is vital that the controller knows exactly what personal data the company processes and why". The deciding factor is the purpose. *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 25.

loss, destruction or damage is included[562]. Integrity is the "property of accuracy and completeness" of personal data, while confidentiality refers to the "property that information is not made available or disclosed to unauthorized individuals, entities, or processes"[563]. Another typical security principle is availability, which is the "property of being accessible and usable on demand by an authorized entity" and it constitutes with the others the CIA triad. For these principles the measures are mainly designed in accordance with Article 32 on security of processing[564].

As previously noted for PbD, DPbD aims at proactively preventing data breaches from occurring. An information security policy should be defined at the organisational level and technical measures should be implemented in order to safeguard the security of the processing. Taking into account the specific circumstances of the processing, security measures could include pseudonymisation and encryption[565]. Moreover, secure transmission of data and authentication and authorisation tools prevent unauthorised access to personal data. Typical measures for security of processing are using "information security management system", "access control management", "intrusion detection and prevention system", performing a security risk assessment, keeping backups and logs, and defining incident response policies and notification procedures[566].

The last principle of Article 5 is accountability. This principle reminds the controller that the principles should be taken seriously because the subject is responsible for, and shall be able to demonstrate compliance, with them. Internal controls and allocation of responsibilities and duties should be defined, and documentation on measures, policies and procedures should be maintained as evidence[567]. Procedures for responding to DPA's or law enforcement's requests should be defined in advance.

562 *See* Article 5(1)(f) GDPR.

563 *See* these definitions in the recognised international standard ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary.

564 *See* Section 2.5.1.

565 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 131.

566 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, pp. 26–27. *See* further Chapter 5.

567 *See* Elisa Faccioli and Marco Cassaro. "Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: "accountability" e "privacy by design"". In: *Il Diritto industriale* 6 (2018), pp. 561–566. Generally, on designing for accountability *see* Joris Hulstijn and Brigitte Burgemeestre. "Design for the Values of Accountability and Transparency". In: *Handbook of Ethics, Values, and Techno-*

Designating a data protection officer (DPO) might facilitate compliance[568]. According to Docksey, accountability is one of the central pillars of the GDPR and one of its most significant innovations[569]. This principle is linked with Article 24 on responsibility of the controller that requires the controller to implement organisational and technical measures, including data protection policies, in order to ensure and be able to demonstrate that processing is performed in accordance with the GDPR[570]. However, accountability means more than responsibility, it is a "proactive and demonstrable responsibility", which also refers to transparency and liability, meaning that the controller should actively develop compliance and be able to demonstrate it[571]. The legal provision of Article 5(2) only mentions the controller, but it is arguable that the processor is accountable as well[572].

Stalla-Bourdillon *et al.* defined a DPbD workflow from the analysis of Article 5 by deriving eight nodes[573]. The first and second nodes are defying the purpose for data sharing and identifying the legal basis. Then, the controller should determine which data are necessary for that purpose (third node) and reduce a non-essential processing activity within the amount of data (fourth node). A data retention period should be set (fifth node) and the accuracy should be ensured (sixth node). The data controller should verify if the processing is fair in the DPbD workflow and if data

---

*logical Design: Sources, Theory, Values and Application Domains*. Springer, 2015, pp. 303–333. ISBN: 9789400769700. Auditing has a pivotal role for compliance.

568 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 135.

569 Docksey, "Chapter IV Controller and Processor (Articles 24–43). Article 24. Responsibility of the controller", p. 557. This study investigates the precursors of accountability in EU legislation, in several international instruments, and even national developments.

570 Article 24 GDPR. For the text *see supra* note no. 380.

571 Docksey, "Chapter IV Controller and Processor (Articles 24–43). Article 24. Responsibility of the controller", p. 561. *See* also Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*, p. 26, which refers to awareness and reliability; Giusella Finocchiaro. "Il principio di *accountability*". In: *Giurispudenza Italiana* 171.12 (2019), pp. 2778–2782, which investigates the meaning of the term in the GDPR.

572 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 136.

573 *See* Sophie Stalla-Bourdillon et al. "Data protection by design: building the foundations of trustworthy data sharing". In: *Data & Policy* 2 (2020), e4, 1–10, e4–5.

are not altered or disclosed without permission to maintain confidentiality (seventh node). Finally, the controller should ensure a transparent and monitored processing (eighth node).

Article 25 also refers to the safeguards that shall be adopted for protecting rights. Chapter III of the GDPR is dedicated to the rights of the data subject, which are exercised based on a request[574]. These rights can be summarised as reported in the following Table 2.3[575].

*Table 2.3 Data subject's rights*

| RIGHT | DEFINITION |
|---|---|
| Right to be informed | Data subject has the right to obtain information |
| Right to access | Data subject has the right to access personal data and obtain certain related information |
| Right to rectification | Data subject has the right to obtain rectification of inaccurate or incomplete personal data |
| Right to erasure | Data subject has the right to obtain erasure of personal data in certain circumstances |
| Right to restriction | Data subject has the right to obtain temporarily restriction of processing |
| Right to data portability | Data subject has the right to receive personal data and have it ported to another controller under some circumstances |

574 *See* Articles 12–22 GDPR.

575 Generally on data subject's rights *see* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, pp. 206–248; Cuffaro, D'Orazio, and Ricciuto, *I dati personali nel diritto europeo*, pp. 327-352; Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, pp. 141–185; Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, pp. 179–250; Bolognini, Pelino, and Bistolfi, *Il regolamento privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati, in vigore da maggio 2016*, pp. 171–276.

| RIGHT | DEFINITION |
|---|---|
| Right to object | Data subject has the right to object to processing on some grounds |
| Right to have human intervention | Data subject has the right to not be subjected to a decision based solely on automated processing that has effects and the right to obtain human intervention and to contest that decision |

Generally, the controller should be aware of the existence of the different types of rights. The data controller should then define procedures and implement measures for handling the data subject's requests to exercise these rights, even by electronic means. Mechanisms to provide control to the data subject over personal data should be envisioned[576]. The requests shall be free of charge, unless they are manifestly unfounded or excessive[577].

Articles 12, 13 and 14 establish the right to be informed and the procedures for transparent and complete communication with the data subject[578]. Privacy policy shall be aligned with the legal requirements that list the specific information to be provided[579]. Machine-readable icons could

576 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 175.

577 *See* further Article 12(5) GDPR.

578 Actually, Article 12 aims to ensure the efficient exercise of information rights by providing for procedures, but it does not lay down a substantive right. The rights are defined in Articles 13 and 14. *See* Radim Polcˇák. "Chapter III Rights of the Data Subject (Articles 12–23). Article 12. Transparency information, communication and modalities for the exercise of the rights of the data subject". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 398–412. ISBN: 9780198826491, pp. 401–402.

579 The elements that have to be provided are defined in Article 13 and 14 GDPR. The former lists the information required where personal data are collected from the data subject, while the latter where personal data have not been obtained from the data subject. The elements that they have in common are: the identity and the contact details of the controller and, where applicable, of the controller's representative; the contact details of the DPO, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the recipients and, if applicable, transfer to a third country; the data retention period or criteria for determining it; the existence of rights (15–20 GDPR) and of the possibility of withdrawing consent; the right to lodge a complaint to a DPA; the existence of automated

be used to give an overview of the processing in an easily visible, intelligible and clearly legible manner[580]. This right is related to the transparency principle described above. Completeness and accuracy of information in the processing activities are of paramount importance for exercising all the other rights of the data subject[581]. Consent forms, privacy policies, and

---

decision making, including profiling, and information about the logic involved. On Article 13 *see* Gabriela Zanfir-Fortuna. "Chapter III Rights of the Data Subject (Articles 12–23). Article 13. Information to be provided where personal data are collected from the data subject". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 413–433. ISBN: 9780198826491. According to this chapter, it is important to stress that the obligation to provide information applies to all processing activities irrespective of the legal basis. On Article 14 *see* Gabriela Zanfir-Fortuna. "Chapter III Rights of the Data Subject (Articles 12–23). Article 14. Information to be provided where personal data have not been obtained from the data subject". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 434–448. ISBN: 9780198826491. Providing the information when personal data are not obtained from the data subject is really important for notifying of the existence of the processing despite the absence of a direct contact between the subject and the data controller.

580 *See* Article 6(7) GDPR. On privacy icons *see* Arianna Rossi and Monica Palmirani. "What's in an Icon?" In: *Data Protection and Privacy: Data Protection and Democracy*. Hart Publishing, 2020, pp. 59–92. ISBN: 9781509932740. The authors explained that privacy policies are rarely read and poorly understood by data subjects. For this reason, this work proposed an icon set that follows the legal design methodology. On this methodology *see* the work of the Director of the Legal Design Lab based at Stanford Law School, Margaret Hagan. "Design Comes to the Law School". In: *Modernising Legal Education*. Cambridge University Press, 2020, pp. 109–125. ISBN: 9781108663311. On legal design *see* also Margaret Hagan. "Legal Design as a Thing: A Theory of Change and a Set of Methods to Craft a Human-Centered Legal System". In: *Design Issues* 36.3 (2020), pp. 3–15; Arianna Rossi et al. "Legal Design Patterns: Towards A New Language for Legal Information Design". In: *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS*. 2019, pp. 517–526; Arianna Rossi and Helena Haapio. "Proactive Legal Design: Embedding Values in the Design of Legal Artefacts". In: *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS*. 2019, pp. 537–544.

581 *See* Zanfir-Fortuna, "Chapter III Rights of the Data Subject (Articles 12–23). Article 13. Information to be provided where personal data are collected from the data subject", pp. 415–416, which reported that since the 1980s the right to information has been called a "chief" right. The importance of this right has also been highlighted by the Court of Justice in the case C-201/14 *Bara* under the DPD, where the court ruled: "As the Advocate General observed in point 74 of his Opinion, the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the

costumer information notices should be revised to achieve transparency. In particular, the privacy policies shall be specific to the processing activity, and the language shall be short, plain and direct[582].

Regarding the right to access, the data subject can obtain confirmation of whether and where personal data is being processed and have access to data. Article 15 GDPR also lists the information to be supplied after an access request. The right to access also entails the right to obtain a copy of personal data[583]. The request can be made by electronic means; thus, within one month of receipt of the request, personal data shall be provided by electronic means, unless otherwise requested[584]. This right enhances transparency and helps the data subject take control over their personal data since it provides a second more detailed layer of information and allows deeper knowledge of the processing that facilitates the exercise of other rights[585].

The right to rectification is addressed in Article 16 GDPR. The data subject has the right to obtain, without undue delay, rectification of inaccurate personal data or completion of incomplete data. This right is related to the accuracy principle. It has been pointed out that the notion of incompleteness shall be assessed with regard to the purpose of the processing activity since some missing personal data may need to be added[586]. Technical mechanisms could directly allow the data subject to update personal data.

---

exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive".

582 *See* Zanfir-Fortuna, *op. cit.*, pp. 426–427, which suggested avoiding legal constructions in the policies and the use of the words "may" and "could". The policies may even be layered for ease of reading.

583 *See* Articles 15(3) and (4) GDPR.

584 Article 12(3) GDPR.

585 Gabriela Zanfir-Fortuna. "Chapter III Rights of the Data Subject (Articles 12–23). Article 15. Right of access by the data subject". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 449–468. ISBN: 9780198826491, p. 452. The modalities for the exercise of the right to access are provided by Article 12 GDPR.

586 Cécile De Terwangne. "Chapter III Rights of the Data Subject (Articles 12–23). Article 16. Right to rectification". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 469–474. ISBN: 9780198826491, p. 473. This chapter even referred to this right as "the right to add missing elements instead of to correct existing data".

Moreover, the right to erasure or "to be forgotten" entails the erasure of personal data based on certain specified grounds[587]. The legal requirement lists five full-prevalence clauses where the right does not apply. However, where applicable, the controller that has made the personal data public shall take reasonable steps, including technical measures and taking into account available technology and the cost of implementation, in order to inform upon request the other controllers which are processing that personal data[588].

With the exercise of the right to restriction the data subject can obtain a temporary restriction of processing where one of the four defined conditions applies[589]. Some methods for restriction are "temporarily moving the

587 *See* Article 17 GDPR. On this right *see* also the CJEU case law. In particular, as a leading case *see* C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*. In this famous case, the right to be forgotten is associated with the removal of a link provided by a search engine. This right has to be balanced with the general public's interest in access to information. In this regard *see* Herke Kranenborg. "Chapter III Rights of the Data Subject (Articles 12–23). Article 17. Right to erasure ('right to be forgotten')". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 475–484. ISBN: 9780198826491. On the right to be forgotten *see* Thibault Douville. "Les variations du droit au déréférencement, note sous CJUE 24 sept. 2019 [2 arrêt]". In: *Recueil Dalloz* 7854 (9 2020), pp. 515–522; Oskar Josef Gstrein. "Right to be Forgotten: EU-ropean Data Imperialism, National Privilege, or Universal Human Right?" In: *Review of European Administrative Law* (1 2020), pp. 125–152; Alessandro Palmieri and Roberto Pardolesi. "Polarità estreme: oblio e archivi digitali. Nota a Corte di Cassazione, sez. I civile, ordinanza 27–03–2020, n. 7559". In: *Foro it.* 1570 (parte I 2020) and Alessandro Palmieri and Roberto Pardolesi. "Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google". In: *Nuovi Quaderni del Foro italiano* 1 (2014), pp. 16–33 (which focused on the Italian framework but highlighted the different conceptions of the right to be forgotten in the digital and non-digital contexts); Silvia Martinelli. *Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale*. Vol. 5. Giuffrè Editore, 2017. ISBN: 9788814220661; Vincenzo Zeno Zencovich and Giorgio Resta. *Il diritto all'oblio su Internet dopo la sentenza Google Spain*. Roma TrEpress, 2015. ISBN: 9788897524274; and Franco Pizzetti. *Il caso del diritto all'oblio*. Vol. 2. G. Giappichelli Editore, 2013. ISBN: 9788834828168.

588 *See* Article 17(2) GDPR.

589 *See* Article 18. It should be noted that the legal requirement indirectly refers to some principles: accuracy, lawfulness and purpose limitation. On this right *see* Gloria González Fuster. "Chapter III Rights of the Data Subject (Articles 12–23). Article 18. Right to restriction of processing". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 485–491. ISBN: 9780198826491.

selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website"[590]. The controller has a duty to communicate the exercise of these last three rights to recipients[591].

The right to data portability is a new right set by Article 20 GDPR[592]. The rationales of this right are enhancing informational self-determination, empowering data subjects and promoting competition[593]. The data subject has the right to receive personal data in a structured, commonly used and machine-readable format and transmit it to another controller when the legal basis is the consent, or the contract and the processing is carried out by automated means. Where technically feasible, the transmission could be directly performed by the first controller[594].

Portability requires specific technological implementation[595]. The crucial element is the format of data[596]. As noted by De Hert *et al.*, the efforts imposed upon data controllers are moderate because the GDPR does not establish a duty of developing interoperable formats[597]. The provision does not require a specific standard format. Therefore, if the format is chosen by the first controller, the second controller will have problems with the usability of the personal data. By contrast, if the second controller chooses

590 Recital 67 GDPR.

591 *See* Article 19 GDPR.

592 On this right *see* WP29 Article 29 Working Party. *Guidelines on the right to data portability*. WP242 16/en, 2017.

593 Orla Lynskey. "Chapter III Rights of the Data Subject (Articles 12–23). Article 20. Right to data portability". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 497–507. ISBN: 9780198826491, pp. 499–500.

594 *See* also Recital 68 GDPR.

595 *See* the study by Janis Wong and Tristan Henderson. "The right to data portability in practice: exploring the implications of the technologically neutral GDPR". In: *International Data Privacy Law* 9.3 (2019), pp. 173–191. The authors created a program for making portability requests. They categorised the received file formats and evaluated compliance with the criteria. The results showed that compliance is difficult to achieve. Therefore, they proposed some technical definitions for structured, commonly used and machine readable formats. Only for the last criterion there are widely accepted standards in the market (e.g. XML).

596 *See* Paul De Hert et al. "The right to data portability in the GDPR: Towards user-centric interoperability of digital services". In: *Computer Law & Security Review* 34.2 (2018), pp. 193–203, p. 196.

597 *See* De Hert et al., *op. cit.*, p. 200. This interpretation is in accordance with Recital 68 GDPR.

the format, the first one will have an excessively onerous duty to transmit that format. This right should be seen as an opportunity to create interconnected user-centric platforms and to develop interoperable formats[598]. The data controller shall integrate in the processing the necessary safeguards to protect the right to portability at a technical level.

On some defined grounds the data subject has the right to object to processing[599] and the right to not be subject to a decision based solely on automated processing which produces legal or similarly significant effects[600]. When the processing is solely based on automated means and the legal basis is a contract or explicit consent, the data subject does not have the latter right; nonetheless, the data controller shall implement suitable measures to safeguard the other rights, freedoms and legitimate interests, and the data subject has the right to obtain human intervention for the decision, and to express their point of view on the decision[601].

---

598 *See* De Hert et al., *op. cit.*, p. 202. The authors argued that the right to portability encourages a real competition between providers and the creation of interoperable formats.

599 *See* Article 21 GDPR. *See* Gabriela Zanfir-Fortuna. "Chapter III Rights of the Data Subject (Articles 12–23). Article 21. Right to object and automated individual decision-making". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 508–521. ISBN: 9780198826491.

600 *See* Article 22(1) GDPR. On automated decision-making and profiling *see* WP29 Article 29 Working Party. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. WP251 17/en, 2017; Robert R. Hoffman and Gary Klein. "Explaining explanation, part 1: theoretical foundations". In: *IEEE Intelligent Systems* 32.3 (2017), pp. 68–73; Sandra Wachter, Brent Mittelstadt, and Chris Russell. "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GPDR". In: *Harv. JL & Tech.* 31 (2017), p. 841; Bilyana Petkova and Franziska Boehm. "Profiling and the Essence of the Right to Data Protection". In: *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 2018, pp. 285–300. ISBN: 9781316831960; Margot E Kaminski. "The right to explanation, explained". In: *Berkeley Tech. LJ* 34 (2019), p. 189; Elena Gil González and Paul de Hert. "Understanding the legal provisions that allow processing and profiling of personal data — an analysis of GDPR provisions and principles". In: *Era Forum*. Vol. 19. 4. Springer. 2019, pp. 597–621; Sandra Wachter, Brent Mittelstadt, and Luciano Floridi. "Why a right to explanation of automated decision-making does not exist in the general data protection regulation". In: *International Data Privacy Law* 7.2 (2017), pp. 76–99.

601 *See* Article 22(2) – (3) GDPR. On automated decision making *see* also Lee A. Bygrave. "Chapter III Rights of the Data Subject (Articles 12–23). Article 22. Right to automated individual decision-making, including profiling". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford Univer-

While providing some guidance on Article 22, Article 29 Working Party created a list of measures that represent good practices when making solely automated decisions, including profiling[602].

This section has attempted to show the implications for implementing data protection principles and integrating safeguards for the rights. Each provision implies an implementation measure be it organisational or technical. More concrete suggestions will be provided in the next Chapters.

So far, this section has focused on the first paragraph of Article 25. The analysis has explained the factors and the core duties embedded in the DPbD principle. The following section will investigate the second part of the provision that provides the DPbDf requirement.

### 2.4.9 Data protection by default

Even though Cavoukian's formulation of the Seven Foundational Principles embeds a default principle in the PbD approach, the GDPR distinguishes between DPbD and DPbDf[603]. Article 25(2) on data protection by default establishes that:

> "2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

Data protection by default is a new obligation for the data controller. Article 25(2) mandates that the controller shall implement appropriate technical and organisational measures as default settings to ensure that

---

sity Press, 2020, pp. 522–542. ISBN: 9780198826491; Guido Noto La Diega. "Against the Dehumanisation of Decision-Making". In: *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 9 (2018), pp. 3–33; Isak Mendoza and Lee A. Bygrave. "The right not to be subject to automated decisions based on profiling". In: *EU Internet Law*. Springer, 2017, pp. 77–98. ISBN: 9783319649559.

602 *See* Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 32.

603 *See* Calzolaio, "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679".

the processing does not include personal data that are not necessary for the specific purpose. This is applicable to "the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility" for each purpose of the processing.

In particular, the term "amount" relates both to the volume of personal data and the types, categories and level of details (i.e. granularity)[604]. The reference to the period of storage requires that if personal data is not needed after an operation for the primary purpose or the secondary and compatible purpose, it shall be deleted or anonymised by default[605].

The measures mentioned shall ensure that by default personal data are not accessible to an indefinite number of natural persons. Therefore, personal data cannot be made public or be disseminated by default. Access is limited to a finite number of natural persons. It has been argued that the wording "indefinite number" refers to a number "larger than the data subject intended or would have reasonably expected"[606].

The arguments presented earlier for identifying the subjects and on the appropriate criterion are valid for DPbDf, too. In this provision the principles and rights highlighted are: purpose specification, data minimisation, storage limitation and the right to access by the data subject[607]. The data controller should collect by default only necessary data that is adequate and relevant for the purpose, which should be specified, explicit

---

604 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 12. Point 49 states: "Controllers should consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of integrity and confidentiality, data minimisation and storage limitation when collecting large amounts of detailed personal data, and compare it to the reduction in risks when collecting smaller amounts and/or less detailed information about data subjects. In any case, the default setting shall not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data are unnecessary or if detailed data isn't needed because less granular data is sufficient, then any surplus personal data shall not be collected".

605 *See* European Data Protection Board, *op. cit.*, p. 13.

606 Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 186.

607 *See* the interesting analysis on data protection by default in D'Acquisto et al., *Intelligenza artificiale, protezione dei dati personali e regolazione*, p. 133.

608 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 186.

and legitimate[608]. Since DPbDf refers to accessibility, it is also linked to the principles of transparency, integrity and confidentiality[609].

The EDPS pointed out that the obligation of Article 25(2) seems to be implicit in the purpose limitation and minimisation principles. Despite this argument, the authority argued that the requirement has another rationale. The provision stresses the importance of the expectations of the data subjects in the sense that their personal data should not be processed "for other purposes than what the product or service is basically and strictly meant to do, leaving by default any further use turned off"[610].

Thus, the amount of personal data should correspond with the data strictly necessary to the basic functions of a product or service. Default settings should be friendly by default. With privacy-friendly default settings the user does not have "to change the settings of a service or product upon the first use" in order to be protected at a maximum level, meaning that the user avoids a difficult procedure and saves time[611].

According to ENISA, the default settings determine how the systems works if nothing is changed[612]. In order to comply with the obligation of the GDPR, the amount of personal data should be the minimum for the purpose, the processing activities should be minimised according to the same purpose, the timing of data storage should be limited as much as possible, as should the accessibility[613]. It is clear that the necessity principle

609 *See* Hansen et al., *Recommendations on shaping technology according to GDPR provision. Exploring the notion of data protection by default*, p. 12.

610 These are the words in European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 7.

611 *See* Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, p. 63.

612 *See* Hansen et al., *Recommendations on shaping technology according to GDPR provision. Exploring the notion of data protection by default*, p. 11.

613 *See ibid.* The Agency identified these four criteria that should be used by data controllers. The fist criterion refers to the minimum amount of data. The number of attributes, sensitive data and identifiable information items should be reduced. The second criterion indicates that the extent of the processing should be minimal in relation to each purpose. The controller should verify whether the operation is necessary for the purpose. The period of the storage should be minimum, too. This third criterion requires a defined storage, so as to limit copies, do no storage at all, or anonymise or erase as soon as possible. Finally, the fourth criterion limits the accessibility of personal data at the minimum level by organisational and technical strategies. Access should be limited by assigned access rights, or by encryption. The location of the storage and who are the recipients are important elements.

plays a central role[614]. In order to enhance transparency, the data subject should be informed of the properties of the default settings as well as the effects of changes[615].

The two requirements of Article 25 are different. DPbD is wider than the "by default" requirement, which is focused on data minimisation and confidentiality[616]. Furthermore, Article 25(2) is expressed in absolute terms without the conditions of the first paragraph[617]. It has thus been suggested that DPbDf presupposes DPbD[618].

Data protection by default is a methodology that applies before the beginning of any processing: the automatism required by the norm is feasible at the development stage especially[619]. In this sense, more importance to the "design stage" is given by paragraph 2 of Article 25 than by the first one. Also reading the norm alongside Recital 78, developers are indirectly forced to design properly by default[620]. This indirect effect should not be underestimated in the market[621]. DPbDf is especially relevant whenever the default settings can be changed by the user[622].

The measures for implementing DPbD and DPbDf could potentially overlap (e.g. in the case of minimisation and storage limitation)[623]. According to the EDPB, these two principles and obligations are "complementary

614 *See* Hansen et al., *op. cit.*, p. 34. The user should intervene for everything that is in addition to what is necessary for the specific purpose.

615 *See* Hansen et al., *op. cit.*, p. 19; and Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 185.

616 Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements", p. 116; Bygrave, "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default", p. 577.

617 *See* Hansen et al., *Recommendations on shaping technology according to GDPR provision. Exploring the notion of data protection by default*, p. 14.

618 *See* Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", p. 183.

619 *See* D'Acquisto et al., *Intelligenza artificiale, protezione dei dati personali e regolazione*, p. 112. The authors noted that DPbD requires a constant attention to the measures, while data protection by default applies before the processing automatically.

620 *See* D'Acquisto et al., *op. cit.*, pp. 114–115. According to this study, data protection by default could assume a prominent role in the future. It will have more importance than DPbD because it directly entails the design of the technologies and how they automatically process personal data.

621 *See* Hansen et al., *Recommendations on shaping technology according to GDPR provision. Exploring the notion of data protection by default*, p. 15.

622 Hansen et al., *op. cit.*, p. 13.

623 *See* Hansen et al., *op. cit.*, p. 22.

concepts, which mutually reinforce each other"[624]. The controller should bear in mind both distinct principles, and then follow them by adopting a holistic approach in the data processing. Indeed, the GDPR requires a "data protection first" approach, as will be shown in the next sections on the other requirements linked to Article 25.

### *2.5 The related provisions of the GDPR*

Under the GDPR several instruments promote compliance. The implementation of Article 25 should be coordinated with other rules that the GDPR sets out.

Primarily, it should be pointed out that the legal requirements on security of personal data facilitate and enhance compliance. Moreover, in certain situations, a DPO shall be appointed, a record of the processing shall be maintained, a DPIA shall be performed, codes of conduct could be adopted, and certification mechanisms, seals and marks could be established[625].

In some cases, the controller and the processor designate a DPO[626]. Among the tasks of this officer is monitoring compliance with the data protection law and with internal policies[627]. Therefore, where designated the DPO shall provide advice on and monitor the DPbD implementation[628]. According to Article 29 Working Party, the DPO plays a key role

---

624 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, point 5, which also noted: "Data subjects will benefit more from data protection by default if data protection by design is concurrently implemented – and vice versa".

625 *See* respectively Articles 37–39, 30, 35, 40–43 GDPR.

626 Article 37 GDPR mandates the appointment in any case where: "(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10". The Union or Member State law may require the designation in other cases.

627 *See* Article 39(1)(b) GDPR.

628 The DPO should have specific skills and expertise in the data protection field. *See* e.g. the standard UNI 11697:2017, which defines the professional profiles at the UNI web store.

in fostering a data protection culture within the organisation and promoting DPbD implementation[629].

The DPbD measures are not indicated in the list of necessary information that the controller shall record in accordance with Article 30 GDPR[630]. However, recording the processing activities is an organisational measure that may support DPbD.

Codes of conduct can contribute to the application of Article 25 GDPR by specifying some measures and procedures referred to in this provision[631]. As explained in the EDPB's guidelines, codes of conduct are "voluntary accountability tools which set out specific data protection rules for categories on controllers and processors", providing a "detailed description of what is appropriate, legal and ethical" in a sector[632]. According to Article 40, these codes are prepared "by associations and other bodies representing categories of controllers and processors". The compliance with such a code is monitored in accordance with Article 41[633]. In the following subsections the analysis will investigate in detail the rules that are more directly connected with Article 25: security measures, DPIA and certification mechanisms.

### 2.5.1 Security measures

The GDPR mandates the implementation of appropriate technical and organisational measures in order to ensure a secure processing of personal data, that protect against unauthorised or unlawful operations and against accidental loss, destruction or damage. The Second Section of Chapter IV of the GDPR is dedicated to the security of processing. Article 32 is the central provision[634]. In this part, the GDPR sets out the rules on

629 *See* WP29 Article 29 Working Party. *Guidelines on Data Protection Officers ('DPOs')*. WP243 17/en, 2017, p. 12.

630 *See* Article 30(1)(a) – (g).

631 Article 40(2)(h) GDPR.

632 EDPB European Data Protection Board. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*. European Data Protection Board, 2019, p. 7.

633 *See* the long Article 41. In particular, an independent and accredited body monitors compliance with a code.

634 On Article 32 *see* Cédric Burton. "Chapter IV Controller and Processor (Articles 24–43). Article 32. Security of processing". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 630–639. ISBN: 9780198826491.

notification of a personal data breach to the DPA and on communication of the breach to the data subject[635].

The text of Article 32 on security of processing begins with the same words as Article 25[636]. Nonetheless, Article 32 refers to the principle of "integrity and confidentiality". Article 25 aims instead to implement all principles of Article 5.

For implementing appropriate security measures, the risk assessment is crucial[637]. After the description of the processing, the potential effects on the rights and freedoms can be identified through the following steps of the risk assessment[638]:

– Identifying the potential effects on the rights and freedoms of individuals in relation to illegitimate access to data, unwanted modification of data and temporary or definitive unavailability of data;

635 Articles 33 and 34 GDPR. As regards notification, *see* European Data Protection Board, *Guidelines 1/2021 on Examples regarding Data Breach Notification*; WP29 Article 29 Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. WP250 18/en, 2018.

636 Article 32 (1) GDPR: "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (...)."

637 *See* Recital 83 GDPR: "in order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage". Article 32 (2) reads as follows: "2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed".

638 *See* CNIL. Commission Nationale de l'Informatique et des Libertés. *The CNIL's Guide on Security of personal data*. 2018, pp. 3–4; European Union Agency for Network & Information Security, *Handbook on Security of Personal Data Processing*.

– Identifying the human or non-human, internal or external sources of risks;
– Identifying the possible threats;
– Evaluating the severity and likelihood of the risks;
– Determining the measures to address the security risks.

When determining the measures, the state of the art shall be evaluated, as well as the cost of implementation and the specific characteristics of the processing activities[639]. Appropriate security measures should be implemented and documented, and periodical security audits should be carried out. Internal guidelines on notifications and procedures in case of data breach are secure organisational measures.

Article 32 explicitly adds the obligation for the processor, lists several examples of security measures, and refers to certification and codes of conduct as mechanisms to ensure compliance[640]. Within the list, pseudonymisation and encryption are methods to ensure security. The contract between the controller and the processor shows that the latter must take all measures pursuant to Article 32 in order to cooperate with the former[641].

The measures implemented according to Articles 25 and 32 are strictly connected and, therefore, it seems difficult to discriminate between technical DPbD measures and security measures[642]. Indeed, the texts of the provisions are similar and DPbD measures should aim at implementing data protection rules within the security principle (i.e. integrity and confidentiality).

However, DPbD obligation and the duty of security represent separate duties with different timing: the former shall be adopted both at the time of the determination of the means for processing and at the time of the

639 On the state of the art of security measures *see* IT Security Association Germany, *Guidelines "State of the Art"*, pp. 18–36.

640 Article 32(1) GDPR refers to these appropriate measures: "(a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing". Article 32(3) provides that "adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance".

641 Article 28(3)(c) GDPR.

642 *See* D'Acquisto et al., *Intelligenza artificiale, protezione dei dati personali e regolazione*, p. 109.

processing itself, while the latter at the time of the processing. Article 25 is inside Chapter IV, Section 1 on the general obligation of the controller and processor. It is explicitly a general and enforceable legal obligation. By contrast, Article 32 is in the next Section 2 on the security of processing, where the duty of security is not defined as an obligation. Despite the categorisation, compliance with Article 32 is backed by the same administrative fines provided for Article 25 in accordance with Article 83(4)(a) GDPR.

### 2.5.2 Data protection impact assessment

The DPIA is a specific assessment mandated by the GDPR. This process aims to identify and minimise the risks for data subject posed by processing. The operations on personal data present some inherent risks for individuals that depend on the nature and scope of processing[643]. It has been argued that data processing raises risks by default[644].

On some grounds conducting a DPIA is mandatory before the beginning of the processing, that is *ex ante*. In particular, Article 35 GDPR requires the controller to carry out an assessment of the impact of the envisaged processing operations or set of similar operations where, taking into account the nature, scope, context and purposes of the processing, its operation is likely to result in a high risk to the rights and freedoms of natural persons[645].

In addition to the general clause, the same legal requirement specifies three cases where the DPIA is particularly required[646]. After a consultation

643 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 179.

644 Katerina Demetzou. "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation". In: *Computer Law & Security Review* 35.6 (2019), p. 105342.

645 Article 35(1) GDPR. *See* also Recitals 84, and 90 – 93 GDPR. On Article 35 *see* Eleni Kosta. "Chapter IV Controller and Processor (Articles 24–43). Article 35. Data protection impact assessment". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 665–679. ISBN: 9780198826491.

646 Article 35(3) GDPR: "(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in

with the EDPB, each DPA has established a list of the kind of processing operations that are, or are not, subject to the requirement[647].

When designated the DPO should collaborate on the assessment[648]. The involvement of the DPO is highly recommended from the beginning of the assessment since the officer can give constant adequate advice[649]. Even the data subjects or their representatives could advise the controller unless their involvement interferes with the protection of commercial or public interests or the security of processing operations[650].

The GDPR further establishes the minimum features of a DPIA. According to the legal requirement, it is necessary to systematically describe the operations, purposes and, where applicable, legitimate interest of the processing, including the explanation of the necessity and proportionality of these operations in relation to the mentioned purposes[651]. Moreover, it is clearly indispensable to include the assessment of the risks and all the measures envisaged by the controller to address the risks, including all the safeguards and mechanisms adopted to ensure the protection of personal data and to demonstrate compliance, taking into account the rights and legitimate interests of data subjects and other persons concerned[652].

---

Article 9 (1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale". According to Article 29 Working Party, this list is non-exhaustive. *See* Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 9.

647 *See* Article 35(4) and (5) GDPR. In 2019 the EDPB released the 28 opinions on the draft lists of the DPA of each Member State. *See* the website of EDPB at <edpb.europa.eu/our-work-tools/our-documents/topic/ data-protection-impact-assessment-dpia_en>. Last accessed 06/10/2021. For drafting the list, it is necessary to take into account the economic effects of such list for the free movement of personal data within the EU. *See* Article 35(6) GDPR on the consistency mechanism.

648 Article 35(2) GDPR. According to Article 39(1)(c), the DPO shall provide advice on DPIA when requested and monitor the analysis.

649 *See* Atanas Yordanov. "Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation". In: *Eur. Data Prot. L. Rev.* 3 (2017), pp. 486–495, p. 493.

650 Article 35(9) GDPR.

651 *See* Article 35(7)(a) and (b) GDPR.

652 *See* Article 35(7)(c) and (d) GDPR.

Since this assessment is complex, codes of conduct could be considered a useful tool for performing the analysis[653]. Even standards provide guidance on managing the process. Whenever the controller realises that there are high risks and fails to determine the measures, prior consultation with the DPA is required in accordance with Article 36.

After the initial analysis, the DPIA should be reviewed in order to monitor the consistency between the risk assessment and the operations of the processing and to perform new analysis in accordance with new risks[654].

The provision of Article 35 contains vague concepts, such as "large scale". The phrase "likely to result in high risk" is also unclear[655]. Hence, Article 29 Working Party specified nine criteria for identifying where the risk is high[656]. This attribute indicates high likelihood and/or high severity of the hypothetical event objectively assessed by the controller[657].

The decision on whether or not to perform an assessment should be made on a case-by-case basis[658]. Therefore, it should be pointed out that carrying out the DPIA is not mandatory for every processing operation. By contrast, DPbD measures and its internal risk evaluation shall always be implemented. The generic steps of a DPIA may be summarised as follows[659]:

---

653 *See* Article 35(8) GDPR, which states: "compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment".

654 Article 35(11) GDPR.

655 *See* Yordanov, "Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation", p. 490. On the "large scale" criterion *see* further Chapter 3, Section 3.3.3.

656 *See* the criteria in Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, pp. 9–10. One of these criteria is the nature of data when it is sensitive or highly personal.

657 Demetzou, "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation".

658 *See* Yordanov, "Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation", p. 491.

659 This framework has been elaborated on many sources. It is based on Article 35 GDPR, the WP29 Opinion on DPIA, a legal analysis of the GDPR and some sources on the subject that include: ISO/IEC 29134:2017(en) Information technology — Security techniques — Guidelines for privacy impact assessment; Commission Nationale de l'Informatique et des Libertés, *Privacy Impact Assessment (PIA). Methodology*; and Yordanov, "Nature and Ideal Steps of the Data

- Assessment of the necessity of the DPIA;
- Systematic description of the planned processing (nature, scope, context, purpose) for each operation or set of operations, and analysis of the personal data workflow and the assets on which they rely;
- Assessment of the necessity and proportionality of the processing operations in relation to the purposes by checking the compliance with data protection principles;
- Identification of the risks in relation to the rights and freedoms of individuals by evaluating their severity and likelihood;
- Identification of the measures and safeguards to address these risks;
- Where applicable, advice of the DPO, consultation with the data subjects, or prior consultation with the DPA;
- Documentation of the assessment and of the process;
- Periodic review of the assessment.

Several methodologies can assist the controller in carrying out the DPIA[660]. This scheme shows that DPbD planning and DPIA may be strictly connected because they take into account contextual factors and the risks for rights and freedoms. They are both iterative and proactive. Indeed, DPbD and DPIA processes require continuous improvement. Both concepts are aligned with the rationale of the accountability principle, which implies scalability, flexibility and technological neutrality. A correct application of DPbD and DPbDf may make a risk assessment unnecessary in many cases because the risk analysis is already integrated and mitigated[661].

---

Protection Impact Assessment under the General Data Protection Regulation", p. 490.

660 *See* Annex 1 of Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Criteria for an acceptable DPIA are provided in Annex 2. *See* also the framework of CNIL provided in: CNIL Commission Nationale de l'Informatique et des Libertés. *Privacy Impact Assessment (PIA). Knowledge basis*. 2018; Commission Nationale de l'Informatique et des Libertés, *Privacy Impact Assessment (PIA). Methodology*; CNIL Commission Nationale de l'Informatique et des Libertés. *Privacy Impact Assessment (PIA). Templates*. 2018. This framework will be further analysed in Chapter 5, Section 5.4 of this book.

661 *See* e.g. Mantelero, "Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32–39)", p. 308; Mantelero, "La gestione del rischio", p. 470; and Yordanov, "Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation", p. 490.

Since DPbD involves a trade-off of data subjects' rights, DPIA is a potential apt point in the compliance process for considering these trade-offs[662]. DPIA is an organisational strategy. Therefore, this assessment may be an important instrument to comply with the requirements of Article 25[663].

### 2.5.3 Certification mechanisms

The last related requirement to be addressed is the certification mechanism since the third part of Article 25 states:

> "3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article".

Article 42 GDPR introduces certification mechanisms, data protection seals and marks as tools for demonstrating compliance of processing operations. In particular, the long legal requirement provides general rules for third-party certification[664]. This certification mechanism is audited by a third-party independent certification body and is supervised by a DPA[665]. The roles are divided as follows. On the one hand, the certification body assesses the conformity of the product or service with predefined requirements included in a technical standard or in the law and by way of a voluntary and transparent process, and where appropriate issues a certifi-

662 *See* Michael Veale, Reuben Binns, and Jef Ausloos. "When data protection by design and data subject rights clash". In: *International Data Privacy Law* 8.2 (2018), pp. 105–123, p. 117. In this study the authors analysed possible trade-offs (e.g. between control and confidentiality).

663 *See* Yordanov, "Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation", p. 490.

664 *See* for a discussion on Article 42 and 43 GDPR, Irene Kamara and Paul De Hert. "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape". In: *Privacy and data protection seals*. Springer, 2018, pp. 7–34. ISBN: 9789462652286; Ronald Leenes. "Chapter IV Controller and Processor (Articles 24–43). Article 42. Certification". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 732–743. ISBN: 9780198826491; Ronald Leenes. "Chapter IV Controller and Processor (Articles 24–43). Article 43. Certification bodies". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 744–754. ISBN: 9780198826491.

665 Kamara and De Hert, "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape", p. 14.

cate; on the other hand, the competent supervisory authority accredits the body in accordance with some criteria, and has the corrective powers to withdraw the certification, order the body to withdraw, and order it not to issue the certification where the requirements are not or no longer met[666]. The requirements depend on the aims of the certification, the type of product or system and its application area[667].

The typical phases of the assessment are: 1) submission of application by the controller or processor (i.e. interested party); 2) formal application review, evaluation, review, attestation, issuance of certification by the certification body; and 3) surveillance of the DPA[668]. ENISA suggested that the data protection authorities should adopt a common approach on the certification models, criteria and processes[669]. In 2019, the EDPB issued the Guidelines on certification under the GDPR in order to give advice to DPAs, certification bodies, national accreditation bodies, EC, to controllers and processors[670].

The certification mechanism of the GDPR is voluntary. Certification is both a means for demonstrating compliance and a tool for enhancing

666 *See* Article 42, 43 and 58(2)(h) GDPR, and Kamara and De Hert, *op. cit.*, p. 15. According to Article 58 GDPR, DPAs have the power to issue and withdraw certification and corrective power, too. Article 58(3)(f) states that the supervisory authority shall have the authorisation power "to issue certifications and approve criteria of certification in accordance with Article 42(5)". In Article 58(2)(h) it is specified that the authority has the corrective power "to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met".

667 *Ibid.*

668 *See* EDPB European Data Protection Board. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*. European Data Protection Board. Version 3.0, 2019, p. 9. *See* also the scheme in Kamara and De Hert, "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape", p. 15. The author adapted the stages of an international standards to Article 42 GDPR.

669 *See* European Union Agency for Network & Information Security, *Recommendations on European Data Protection Certification*, p. 26.

670 European Data Protection Board, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*.

671 *See* Recital 100 GDPR that states: "in order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services".

transparency[671]. Therefore, certification is linked with the concept of accountability[672].

However, compliance with the GDPR cannot be certified. Article 42(4) explicitly specifies that a certification does not reduce the responsibility of the controller or the processor to comply with the Regulation, leaving intact the judgement of the supervisory authorities or the courts. Thus, certification is not a presumption of full conformity with the legal obligations stemming from the GDPR[673].

Nonetheless, it has been argued that certification is a means for "externalising in a concrete and objective way that technical and organisational measures (or a part of them depending on the scope of the certification) have been taken and implemented in a satisfactory manner"[674]. Moreover, according to Article 83 the DPA takes into account the adherence to an approved certification mechanism when imposing the fines[675].

In accordance with the third paragraphs of Article 25, DPbD may be translated into a certification requirement and its implementation may be certified by an accredited, independent and expert party. As previously noted for PbD, the certification could guide data subjects, it enhances their trust, and represents a competitive advantage in the market. In addition, the EDPB argued that "the ability to get a processing operation certified provides an added value to a controller when choosing between different processing software, hardware, services and/or systems from producers or processors", and that "certification seal may also guide data subjects in their choice between different goods and services"[676]. As a result, developers and providers may be indirectly encouraged to adopt a certification by implementing DPbD and DPbDf so as to obtain a competitive advantage in the market and enhance trust in the processing.

In summary, this section has investigated how the EU legal framework on data protection has established an obligation to regulate by design and by default data processing operations. It is now necessary to compare the concepts of PbD, as described in the critical analysis, and DPbD in order to explain why the wording cannot be used interchangeably.

---

672 *See* European Union Agency for Network & Information Security, *Recommendations on European Data Protection Certification*, p. 13.

673 Kamara and De Hert, "Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape", p. 25.

674 *Ibid.*

675 Article 83(2)(j) GDPR.

676 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 29.

## 2.6 A comparison between privacy and data protection by design

The concept pioneered by Ann Cavoukian differs from the GDPR's principle in many ways. This section explains the similarities and differences between PbD and DPbD.

PbD is usually connected with the FIPs, while DPbD is established in the EU data protection framework. Indeed, it has been argued that the concept of the GDPR is more comprehensive than PbD[677]. As noted above, the FTC pointed out that its framework incorporates the FIPs. DPbD is more ambitious because it goes beyond the FIPs and entails more rights and principles[678]. The EU principles are more wide-ranging than the FIPs, in the US conception especially[679]. For examples, the right to access in the GDPR (Art. 15) and the right to object automated decision making (Art. 22) are not in the FIPs. Thus, DPbD should integrate more safeguards in order to protect these specific rights of the data subject. The EU Charter of Fundamental Rights shall also be included because Article 25 refers to the rights and freedoms after mentioning the GDPR requirements.

Furthermore, both concepts represent broad proactive approaches. PbD is an international concept perceived as a principle and advocated by scholars and policymakers for the protection of privacy and personal data. It includes the protection of default settings. DPbD and DPbDf are separately defined in a legal requirement of a regulation focused on persona data. DPbD is a fully enforceable obligation, while PbD entails a visionary and ethical dimension[680].

The terms cannot be used interchangeably[681]. It has been pointed out that DPbD has been inspired by the concept of PbD[682]. Following the arguments and the lines of the critical analysis performed on PbD, some considerations on DPbD can be made.

It is arguable that Article 25 included a flexible and enforceable rule that is applicable to various contexts in the EU framework for the processing

677 Tsormpatzoudi, Berendt, and Coudert, "Privacy by design: from research and policy to practice–the challenge of multi-disciplinarity", p. 202.
678 Bygrave, "Hardwiring privacy", p. 761.
679 *See ibid.* On the comparison between EU and US principles *see* Chapter 4, Section 4.2.
680 *See* European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, pp. 1, 5.
681 Bygrave, "Hardwiring privacy", p. 761.
682 *See* Luiz Costa and Yves Poullet. "Privacy and the regulation of 2012". In: *Computer Law & Security Review* 28.3 (2012), pp. 254–262, p. 260.

of personal data. However, the requirement has a broad definition that makes it difficult to implement, as previously noted. This provision does not seem clear enough for stakeholders. It does not define standards for the design process and misses the references to developers. Nevertheless, Article 25 is technologically neutral and dynamic and leaves room to specific customised solutions.

DPbD may improve the effectiveness of the GDPR by empowering data subjects. The translation and interpretation issues are still relevant, but several projects are underway to overcome the challenges. With DPbD and DPbDf the EU is promoting a proactive and preventive approach without completely delegating privacy regulation to companies.

DPbD is strictly connected to data security without confusing the approaches. It requires both "privacy-by-policy" and "privacy-by-architecture" strategies. Building data protection principles will not always be possible. However, the GDPR is a set of rules that has to be perceived as a whole. Article 25 is just a piece of the puzzle.

As explained, DPbD implementation demands organisational measures. The data controller in the material and territorial scope of the GDPR should adopt internal processes and bolster privacy management. Withing the GDPR, bureaucratic solutions for data protection are not sufficient for compliance.

Since 25 May 2018 large investments have been made in privacy programmes. It can be argued that DPbD and DPbDf can increase trust and confidence in products and services by creating opportunities for business. The relative concerns should not be forgotten, but the arguments adopted for balancing the disadvantages for PbD can be used here for DPbD.

Moreover, certification opportunity is directly mentioned by Article 25. EDPS explicitly presents DPbD as an opportunity for boosting the respect of ethics in technological development[683]. The GDPR does not aim to create barriers to innovation, but to provide a strong and more coherent data protection framework, backed by enforcement and given the importance of the digital internal market and the free movement of personal data within it[684]. It is hoped that DPbD will contribute to the creation of user-centric technologies and policies without excessively increasing the costs of access to them.

683 European Data Protection Supervisor, *Opinion 5/2018, Preliminary Opinion on privacy by design*, p. 21.

684 *See* Recitals 7 and 13 GDPR.

DPbD is a different version of Cavoukian's PbD. The following Table 2.4 summarises the main results of the comparison between the two concepts.

*Table 2.4 Summary of the comparison between PbD and DPbD*

| CRITERIA | PbD | DPbD |
|---|---|---|
| Legal system | International recognition at policy level | EU |
| Legal nature | Recommended practice | Principle and obligation |
| Theoretical framework | Privacy and data protection | Data protection |
| Embedded principles | FIPs | GDPR principles and EU Charter |
| Embedded rights | Non specified | Arts. 12–22 GDPR and Charter |
| Timing | Full life cycle | Full life cycle of processing |
| Flexibility | Yes | Yes |
| Technical neutrality | Yes | Yes |
| Subjects | All stakeholders | Data controller primarily |
| Privacy by Default | Included | Excluded |
| Security | Included | Separate duty |

Having defined what is meant by PbD, DPbDf and DPbD, and before proceeding to contextualise the latter principle in the healthcare context it is important to discuss the interplay between data protection and other fundamental rights.

## 2.7 Balancing the right to data protection against other rights and freedoms

The human rights discourse plays an increasing role in the debate on digital technologies[685]. The rights to privacy and data protection are not absolute rights. They may be limited, if necessary, to protect a general interest or other rights and freedoms[686]. A synergy between privacy and other legal values is possible, as are conflicts[687]. In society there are typically competing interests at play. In his pioneering book of 1967, Westin defined privacy as follows[688]:

> "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

In Westin's view, privacy is never absolute, and it exists in the context of a relationship between the individual and society. The natural person has control over his or her data. The balances of privacy vary from society to society due to cultural differences[689].

This study focuses primarily on data protection in the EU. According to Recital 4 GDPR, the right to the protection of personal data shall be considered "in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality". As noted above, the GDPR refers to the Charter of Fundamental Rights of the European Union, and in particular to the respect for private and family life, for home and communications, the respect of freedom of thought, of conscience and religion, of freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

According to Article 52(1) of the Charter and the CJEU's case law, limitations to the right of data protection are admissible if all the following conditions are met[690]:

---

685 Sartor, "Human rights and information technologies", p. 434.

686 *See* Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 35; Rodotà and Conti, *Intervista su privacy e libertà*.

687 Sartor, "Human rights and information technologies", p. 442.

688 Westin, *Privacy and Freedom*, p. 7.

689 Westin, *op. cit.*, p. 31.

690 *See* Article 52(1) of the Charter and Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, pp. 42–52. This Handbook also provides some examples of the case law where each condition is further explained by the CJEU.

1. Limitations are provided for by law with sufficient precision;
2. Limitations respect the essence of the right to data protection, meaning that they do not devoid a fundamental right of its basic content without any justification;
3. Limitations are necessary and proportionate. Limitations can apply only in so far as strictly necessary and the resulting advantages do not outweigh the disadvantages that arise for the fundamental rights at stake;
4. Limitations meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

Moreover, Article 23 of the GDPR specifies that possible restrictions provided by law shall respect the essence of the fundamental rights and freedoms and they shall be necessary and proportionate measures in a democratic society in order to safeguard defined general interests, such as national security or the rights and freedoms of others[691]. This Article

691 *See* Article 23 GDPR. The interests to safeguard are: "(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) 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); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims". As regards the need to meet objectives of general interest, they are further defined in Article 3 of the Treaty of the EU and in other specific provisions. Article 3 of the Treaty states that: "1. The Union's aim is to promote peace, its values and the well-being of its peoples. (...) It shall combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men, solidarity between generations and protection of the rights of the child. (…) It shall respect its rich cultural and linguistic diversity, and shall ensure that Europe's cultural heritage is safeguarded and enhanced. (...) 5. In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations

recognises that the right to personal data shall be considered in relation to its function in society[692].

Thus, when striking the balance between the right to data protection and another interest, the solution shall be a prudent and fair balance at the legislative level, which is guided by the constitutional principles of necessity and proportionality[693]. These principles represent a dual requirement with which a legislative measure shall comply[694].

Proportionality and necessity are general principles of EU law that have been widely used in the Court of Justice's case law[695]. In order to assess

---

Charter (...)". *See* the implementation of Article 23 in Member States' legislation at Legal TIPIK. *Report on the implementation of specific provisions of Regulation (EU) 2016/679*. European Commission. Directorate – General for Justice and Consumers, Unit C.3 Data Protection, 2021, pp. 15–23.

692 *See* Dominique Moore. "Chapter III Rights of the Data Subject (Articles 12–23). Article 23. Restrictions". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 543–554. ISBN: 9780198826491, p. 545.

693 On principles of European constitutional law *see* Armin von Bogdandy and Bast Jürgen. *Principles of European Constitutional law*. Hart Publishing, 2020. ISBN: 9781841138220. On striking the balance between constitutional rights *see* Robert Alexy. "Constitutional rights, balancing, and rationality". In: *Ratio Juris* (2003), pp. 131–140; Giorgio Pino. "Conflitto e bilanciamento tra diritti fondamentali. Una mappa dei problemi". In: *Ragion Pratica* 28 (2007), pp. 219–276; Pino, *Diritti e interpretazione. Il ragionamento giuridico nello Stato costituzionale*; Robert Alexy. *A theory of constitutional rights*. Oxford University Press, 2010. ISBN: 9780199584239; Riccardo Guastini. "Principi costituzionali: identificazione, interpretazione, ponderazione, concretizzazione". In: *Dialoghi con Guido Alpa. Un volume offerto in occasione del suo LXXI compleanno*. 2018, pp. 313–324. ISBN: 9788832136050.

694 *See* EDPS European Data Protection Supervisor. *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*. European Data Protection Supervisor, 2019, p. 2.

695 *See* the analysis by Lynskey, *The foundations of EU data protection law*, which dedicates Chapter 5 to "Reconciling Data Protection with Other Rights and Interests". *See* also Bogdandy and Jürgen, *Principles of European Constitutional law*, pp. 505–512 Charlotte Bagger Tranberg. "Proportionality and data protection in the case law of the European Court of Justice". In: *International Data Privacy Law* 1.4 (2011), pp. 239–248; Marie-Pierre Granger, Kristina Irion, et al. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection". In: *European Law Review* 39.4 (2014), pp. 835–850; Orla Lynskey. "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland". In: *Common Market Law Review* 51.6 (2014), pp. 1789–1811; Jeanne Pia Mifsud Bonnici. "Exploring the non-absolute nature of the right to data protection". In:

the proportionality and necessity of a measure, the legislator may apply two step-by-step methodologies: the so-called "necessity test" and "proportionality test"[696]. In fact, the two principles imply two different tests, and the latter shall follow the former, since necessity is a pre-condition for proportionality[697].

The first analysis is the "necessity test", which describes whether the measure is effective for the objective to be pursued and whether it is less intrusive compared to other options for achieving the same goal[698]. The EDPS listed the four steps of this test as follows[699]:

1. Factually describing in detail the measure proposed;
2. Identifying whether this measure represents a limitation on the rights to privacy and data protection, and to other fundamental rights;
3. Considering the goal of the measure against which the necessity of a measure should be assessed (e.g. public security);
4. Choosing whether the measure is effective and the least intrusive.

Secondly, the "proportionality test" should be performed. According to the CJEU's case law and to the EDPS, the advantages resulting from the legislative and discretionary measure shall not be outweighed by the disadvantages the measure causes with respect to the exercise of fundamental rights[700]. So, the test shall assess what safeguards the measures shall pro-

---

*International Review of Law, Computers & Technology* 28.2 (2014), pp. 131–143; Raphaël Gellert. "Understanding data protection as risk regulation". In: *J. Int. Law* 18.11 (2015), pp. 3–16; Paul De Hert and Vagelis Papakonstantinou. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" In: *Computer law & security review* 32.2 (2016), pp. 179–194.

696 *See* respectively EDPS European Data Protection Supervisor. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*. European Data Protection Supervisor, 2017; European Data Protection Supervisor, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*.

697 On the relationship between necessity and proportionality *see* European Data Protection Supervisor, *op. cit.*, p. 9.

698 European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*, p. 5.

699 *See* European Data Protection Supervisor, *op. cit.*, p. 9, which provides more guidance on each step with reference to the CJEU's case law.

700 European Data Protection Supervisor, *op. cit.* In particular, the authority highlights the ruling of the CJEU in the Digital Rights Ireland case. The reference is: Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Judgement of the Court (Grand Chamber) of 8 April 2014. Joined Cases C-293/12 and C-594/12.

vide in a particular context in order to reduce the risks for the rights to a proportionate level. The four steps are[701]:

5. Assessing the legitimacy of the goal of the measure proposed and whether this measure genuinely meets this goal from an "advantage/benefit" point of view[702];
6. Assessing the scope, extent and intensity of the impact to the rights from a "disadvantage/cost" point of view;
7. Proceeding to a fair balance between the two previous points of view;
8. Taking a decision on the proposed measure[703]. If the measure is not proportionate, introducing safeguards is fundamental.

Looking at these tests, the "goal" of the measure is usually the protection of the competing right or interest. Actually, the right to data protection interacts with several rights. For example, a balance of free speech and data protection interests is the de-indexing information required by the right to be forgotten[704]. In Article 85, the GDPR explicitly refers to the rights to freedom of expression and to receive information stating that Member States shall reconcile the right to the protection of personal data with these other rights[705].

---

701 European Data Protection Supervisor, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, p. 12.

702 This phase is called "suitability" and "in fact test" by Bogdandy and Jürgen, *Principles of European Constitutional law*, p. 506.

703 This is the so-called "proportionality in the narrow sense" phase in Bogdandy and Jürgen, *op. cit.*, p. 507. During the analysis the concept of margin of appreciation is used.

704 *See* Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, p. 80. *See* also the analysis by Oreste Pollicino. "L'autunno caldo' della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale". In: *Federalismi.it* 19 (2019), pp. 2–15, which focuses on how the CJEU decided in its case law and how its decisions impacted the global digital market.

705 On the balance between privacy, data protection and freedom of expression *see* Christopher Docksey. "Four fundamental rights: finding the balance". In: *International Data Privacy Law* 6.3 (2016), pp. 195–209; Stefan Kulk and Frederik Zuiderveen Borgesius. "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe". In: *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 2018, pp. 301–320. ISBN: 9781316831960; Giorgia Bincoletto. "Italy – Italian DPA Balancing Data Protection and Freedom of Expression: Essentiality and Fairness as key principles". In *Eur. Data Prot. L. Rev.* 7 (1 2021), pp. 115–119. On this right in the digital age *see* Giovanni Pitruzzella, Oreste Pollicino, and Stefano Quintarelli. *Parole e potere: libertà d'espressione, hate speech e fake news*. EGEA, 2017. ISBN: 9788823836419.

For the purposes of the present research, it is not necessary to discuss all the possible interactions of the right to data protection. Indeed, it is relevant to stress that when advocating the respect of DPbD and DPbDf, possible conditions may limit the right to data protection, and some balancing may be necessary[706]. This balancing results in an equilibrium between two rights or interests that avoids the sacrifice of one in favour of the other[707].

Generally, DPbD establishes a balance between competing interests by indicating the factors and criteria analysed above, such as the cost of implementation and the risks for rights and freedoms. As explained, a weighing process is already embedded in Article 25.

However, the obligation to implement DPbD could significantly affect the economic interests of the controller, which is recognised under freedom to conduct a business[708]. Whether the economic interests of private parties, or of the general public in the case of public tenders, could justify limiting the right to data protection is a general question[709]. According to some scholars, this interaction is a so-called "partial conflict" because a case-by-case approach is possible[710]. It is necessary to bear in mind that "data protection readjusts the balance of power between the data subject and those who process personal data", and it "reduces power asymmetry through the use of opt-in as a default setting"[711]. Within DPbD the law is responsive to the power of design by articulating boundaries, guidance, and goals to innovation[712]. As noted in the beginning of this book, design is powerful and political[713]. Striking the balance between the right to data protection and freedom to conduct a business may apply the general rules outlined above, but the concrete choice does not come from the

706 On balancing rights and the tasks of the courts and legislators *see* Giovanella, *Copyright and Information Privacy: Conflicting Rights in Balance*.

707 *See* Giovanella, *op. cit.*, p. 11. The author explains that she prefers the term "right", but the term "interest" is also frequently used by scholars.

708 Article 16 of the Charter of Fundamental Rights of the European Union states: "the freedom to conduct a business in accordance with Union law and national laws and practices is recognised".

709 Giakoumopoulos, Buttarelli, and O'Flamerty, *Handbook on European data protection law*, p. 78.

710 *See* further in Giovanella, *Copyright and Information Privacy: Conflicting Rights in Balance*, p. 8.

711 Lynskey, *The foundations of EU data protection law*, pp. 213, 214.

712 Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, p. 51.

713 *See* the Introductory Remarks.

legislator, but from the data controller, and (maybe) from the developer. The EU legislator introduced the "state of the art" and the "cost of implementation" criteria for providing concrete factors and some guidance for DPbD implementation. Nonetheless, courts and the DPAs while ruling on future case law will probably define more detailed steps for balancing these specific interests embedded in Article 25 GDPR.

In addition to the interests of the data controller, the implementation of DPbD in a specific context could create a conflict between the interests of the individual for the protection of his or her rights and freedoms, which are better guaranteed by design or by default, and of the public, which may want to use personal data for protecting substantial or general interests. A particular context where the protection of personal data under Article 25 may conflict with other public interests is the healthcare domain since personal health data may be used in the area of public health for protecting communities and societies against serious threats to health (e.g. pandemic), for conducting scientific research, or for ensuring high standards of health management. So, balances, necessary goals and exceptions, and proportionate safeguards may be needed in some situations. Also, for this reason, this work investigates the significance of DPbD in a specific field of the healthcare domain, which is e-health. More considerations on striking the balance between data protection and public health will be added at the end of the next Chapter.

Thus far, specific case law on the inner balance of Article 25 does not exist, but DPAs have started to sanction data controllers for non-compliance with its requirements[714]. It is arguable that future court rulings, and legislative measures will better specify how to balance the principle of DPbD and the right to data protection against other principles, rights and interests, especially. The fair balance will remain a necessary task of courts and legislators. In summary, this Chapter has attempted to provide a deep analysis of PbD and DPbD.

As pointed out by Tamó, the concrete implementation of these approaches depends on the actual technology at play, the sector where it is used and the context of the individual case[715]. The Chapter that follows moves on to consider the e-health field and the processing of personal health data, analysing the legal framework and presenting a case study of e-health technology: the Electronic Health Record system.

---

714 *See* Chapter 6, Section 6.5.

715 Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, p. 200.