Technology and Regulation

A Brief History of Data Protection by Design

From multilateral security to Article 25(1) GDPR

Pierre Dewitte*

GDPR, Accountability, Responsibility, Data protection by design, Historical analysis

Article 25(1) of the General Data Protection Regulation ("GDPR") is the first provision that comes to mind when discussing data protection by design. Yet, the origins of that concept can be traced back to an idea that was already solidly established in the software engineering community before its adoption. Besides, the GDPR is not the first binding piece of legislation that incorporates such an obligation. This paper is the first part of a two paper series that explores the history of data protection by design and its manifestation in the text of the GDPR. This first paper unravels the history of that concept by delving into its technical roots and outlining the national and EU initiatives that have preceded the GDPR. Such a retrospective provides the necessary background for the second paper to delve into the implications and scope of its current manifestation in the text of the Regulation.

pierre.dewitte@kuleuven.be

1. Introduction

"Data protection by design", understood as an approach to integrate privacy and data protection considerations at the earliest stages of the software development lifecycle, has not always been known as such. "Privacy by design", "privacy engineering" and "privacy enhancing technologies", for instance, are still used as catch-all terms to refer to slightly different flavours of a similar idea. Neither has it always been so consciously incorporated in EU law as is the case in Article 25(1) of the General Data Protection Regulation ("GDPR").[1] As audacious as it is, that provision was not pieced together from scratch during the data protection law reform. If the GDPR certainly contributed to promoting the *concept* of data protection by design, its *origins*, however, can be traced back to an idea that was already solidly established in the software engineering community way before the Regulation. The GDPR is not even the first binding piece of legislation that incorporates such an obligation. Rather, Article 25(1) GDPR is but the modern manifestation of a cross-disciplinary concept that has roots in both legal and technical literature.

The GDPR is light on details when it comes to the measures controllers must implement to comply with data protection by design. This is a recurring critique among legal scholars, some of whom have claimed that the vagueness and complexity of Article 25(1) GDPR is an obstacle to its meaningful enforcement.[2] Among the most vocal detractors of Article 25(1), Ari Waldman even argues that the "language used is so vague that the provision [is] rendered meaningless", referring to data protection by design as a "catch-all provision that has no identity of its own".[3] Unravelling the origins of that approach, however, can go a long way in understanding its scope, role and implications. This paper therefore aims to provide a comprehensive overview of the initiatives that have preceded the inclusion of data protection by design in the GDPR. As the first part of a two paper series, it also sets the scene for the second paper to dissect the constitutive elements of Article 25(1) GDPR, and contributes to better grasp the motivations behind the shift from a traditional to a risk-based approach to data protection.[4]

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (ELI: http://data.europa.eu/eli/reg/2016/679/oj).

* Pierre Dewitte, KU Leuven Centre for IT & IP Law

Received 21 Aug 2023, Accepted 24 Sep 2023, Published 25 Oct 2023

2 See, among others, Giorgia Bincoletto, 'A Data Protection by Design Model for Privacy Management in Electronic Health Records' in Maurizio Naldi and others (eds), *Privacy Technologies and Policy* (Springer International Publishing 2019) 161, 168 http://link.springer.com/10.1007/978-3-030-21752-5_11; Bert-Jaap Koops and Ronald Leenes, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the "Privacy by Design" Provision in Data-Protection Law' (2014) 28 *International Review of Law, Computers & Technology* 159, 161 http://www.tandfonline.com/doi/abs/10.1080/13600869.2013.801589; Gerrit Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012' (2012) 9 SCRIPTed 64, 75, and the references in footnote 40 http://www.script-ed.org/?p=406; Seda Gurses, Carmela Troncoso and Claudia Diaz, 'Engineering Privacy by Design' (2011) Unpublished 2 https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf.

3 Ari Ezra Waldman, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53 *Cornell International Law Journal* 147, 149 https://heinonline.org/HOL/P?h=hein.journals/cintl53&i=169.

4 On the risk-based approach, see Raphaël Gellert, 'Understanding the Risk-

Section 2 focuses on the early traces of data protection by design, mainly in the form of technical solutions developed in the software engineering community and covers both the inception of "Privacy Enhancing Technologies" as well as relevant standardisation efforts. Section 3 then details the progressive integration of that concept into the regulatory agenda, both at the national and EU levels. That section goes beyond an overview of the data protection reform process, but also highlights the role of other regulatory frameworks than the GDPR have and are currently playing in the push for a risk-based approach to data protection. Finally, Section 4 rounds up the analysis by outlining the manifestation of data protection by design in the GDPR and delving into its concrete role within that regulatory framework.

Venturing into the past, however, requires at least a general idea of what to look for. The broad definition put forward by the European Union Agency for Cybersecurity ("ENISA") provides a solid starting point for such a retrospective. Acknowledging the divergences of interpretation between lawyers and software engineers, the Agency has described data protection by design as a "process involving various technological and organizational components, which implement privacy and data protection principles by properly and timely deploying technical and organization measures".[5] The following sections leverage that definition as a reference point when scrutinizing the complex history that has led to the adoption of Article 25(1) GDPR. Except when discussing that provision more specifically, this paper uses the notions of "data protection by design" and "privacy by design" interchangeably to refer to the various approaches that fall under the ENISA's broad definition, giving preference to the wording used by the authors of each item under consideration.

2. Its debut in the form of technical solutions

The first occurrence of the term "privacy by design" dates back to the sixties, when it was used in the building and architecture sectors to emphasise the growing importance of *residential* privacy.[6] The concept understood within the meaning of ENISA's definition only gained traction among software engineers some twenty years later to counterweight the rampant development of surveillance technologies, especially in the United States.

2.1 In the beginning were PETs

It is only later, though, that software engineers started to consider technology not only as the *source* of these growing privacy concerns, but also as a viable *solution* to address them. As pointed out by the European Data Protection Supervisor ("EDPS") in its Preliminary Opinion 5/2018 on Privacy by Design,[7] this paved the way for a thriving field of research leveraging advances in computer security, more specifically cryptography, to propose privacy-preserving countermeasures to the risks posed by new information and communication technologies. These technical solutions designed to address privacy issues were soon labelled as "Privacy Enhancing Technologies" ("PETs"), a term still omnipresent years later.

David Chaum pioneered that approach in the early eighties with his seminal work on anonymous communications and untraceable payments.[8] This inspired researchers to broaden the scope of ICT security, so far limited to addressing security risks from a system owner's perspective, to also consider end users' privacy. Referred to as "multilateral security",[9] that approach insisted on the need to break away from the strict conception of ICT security as a way to defend oneself against external attackers and misbehaving users, to also include the design choices made by system owners as potential risk sources. As detailed by Kai Rannenberg, negotiations between all involved parties should play a fundamental role in the design process. This presupposes that users are fully aware of the functioning of the system at stake, and that system operators have implemented features that allow effective control over the main aspects of the processing.[10] And, more than anything else, that those considerations have been thought through as of the design stage. If multilateral security gradually merged with ongoing efforts in the field of PETs, it already contained the seeds of an idea that bloomed throughout the nineties.

Speaking of PETs, some claim that the first usage of the term can be attributed to a report of the Dutch Data Protection Authority and the TNO Physics and Electronics Laboratory issued in 1995 upon request from the Information and Privacy Commissioner of Ontario.[11] This deserves to be nuanced. First, its conceptual roots are to be found much earlier so that techniques that would typically be considered as PETs today pre-date the said report by "well-over a decade".[12] Second, its scope is limited to the technological solutions developed to sepa-

Based Approach to Data Protection: An Analysis of the Links between Law, Regulation, and Risk' (Vrije Universiteit Brussel 2017).

5 Claude Castelluccia and others, 'Data Protection Engineering - From Theory to Practice' (European Union Agency for Cybersecurity 2022) 7 https://www.enisa.europa.eu/publications/data-protection-engineering.

6 Alan Hedley, *Privacy as a factor in residential buildings and site development: an annotated bibliography* (1966, National Research Council of Canada. Division Of Building Research) 12 https://nrc-publications.canada.ca/eng/view/object/?id=f9132094-25cc-480a-8ccc-4b6104b5c458. Mentioned by Simon Davies, 'Why Privacy by Design Is the Next Crucial Step for Privacy Protection' (Initiative for a Competitive Online Marketplace 2010) 1 https://pdfs.semanticscholar.org/7ffc/3255202775711oad60b3ae701148b702f706.pdf.

7 European Data Protection Supervisor, 'Opinion 5/2018 - Preliminary Opinion on Privacy by Design' para 15 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

8 David Chaum, 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms' (1981) 24 Communications of the ACM 84 http://doi.org/10.1145/358549.358563; David Chaum, 'Blind Signatures for Untraceable Payments' in David Chaum, Ronald L Rivest and Alan T Sherman (eds), *Advances in Cryptology* (Springer US 1983) http://link.springer.com/10.1007/978-1-4757-0602-4_18; David Chaum, 'Security Without Identification: Transaction Systems to Make Big Brother Obsolete' (1985) 28 *Communications of the ACM* 1030 http://doi.org/10.1145/4372.4373; David Chaum, Amos Fiat and Moni Naor, 'Untraceable Electronic Cash', *Advances in Cryptology* (Springer 1988) https://link.springer.com/chapter/10.1007/0-387-34799-2_25.

9 See, for an overview and evaluation of technologies for multilateral security: Andreas Pfitzmann, 'Multilateral Security: Enabling Technologies and Their Evaluation', *ETRICS 2006: Emerging Trends in Information and Communication Security* (Springer 2006) https://link.springer.com/chapter/10.1007/11766155_1.

10 See, more specifically, the technical design strategies outlined in Kai Rannenberg, 'Multilateral Security a Concept and Examples for Balanced Security', *Proceedings of the 2000 workshop on New security paradigms* (Association for Computing Machinery 2001) 160-161 http://doi.org/10.1145/366173.366208; See also: Kai Rannenberg, 'Recent Development in Information Technology Security Evaluation - The Need for Evaluation Criteria for Multilateral Security', *Proceedings of the IFIP TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society* (North-Holland Publishing Co 1993) https://dl.acm.org/doi/10.5555/647317.723330.

11 Enterprise Privacy Group, 'Privacy by Design - An Overview of Privacy Enhancing Technologies' (2008) 2 https://www.dsp.utoronto.ca/projects/surveillance/docs/pbd_pets_paper.pdf. See, for the joint report from the Dutch Data Protection Authority and TNO: Registratiekamer, 'Privacy-Enhancing Technologies: The Path to Anonymity - Volume II' (1995) https://silo.tips/download/privacy-enhancing-technologies-the-path-to-anonymity.

12 Enterprise Privacy Group (n 11) 2.

rate the use of the system from the identity of the user. By focusing on anonymisation, it therefore only covers a subset of what is currently understood as PETs. While the origins of that concept remain debated, researchers in the field soon settled on a definition that is still widely used to this day, referring to those technologies as "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".[13]

PETs quickly became part of a broader, prolific field of research under the "privacy engineering" and "privacy by design" umbrellas, with dedicated fora to discuss the most recent developments in these areas.[14] Along PETs emerged an incredibly diverse set of initiatives aiming at integrating privacy and data protection considerations into the traditional software development lifecycle, ranging from privacy design principles, strategies and patterns to *ad-hoc* risks assessment methodologies and privacy-oriented modeling approaches. If a comprehensive overview of the stat of the art would largely exceed the remit of this paper, one could already note that data protection by design cannot be reduced to the implementation of PETs; and neither is it limited to a collection of general principles to be observed by controllers while designing products and systems involving the processing of personal data.[15]

2.2 Parallel standardisation efforts

As personal data processing became an integral part of modern ICT systems, so did the need to consider and mitigate their impact on individuals' privacy. If the authors mentioned above laid the foundations of PETs as a new research track, the diversity of the risks to be addressed combined with the complexity of the solutions to be contemplated called for the development of common technological approaches designed to address recurring issues. It is therefore no surprise that standardisation efforts have played a significant role in the field of privacy, both at the international and EU levels.[16] As a form of self- or co-regulation tools,[17] standards respond to a demand emanating from industry for readily-deployable and widely-accepted solutions to cross-cutting challenges that guarantee a degree of robustness and recognition.

The prolific work of the International Organization for Standardization ("ISO") in proposing concrete technological solutions addressing specific privacy issues must be highlighted. Notable examples of standards include ISO/IEC 29191:2012, ISO/IEC 20889:2018, ISO/IEC 27555:2021 and ISO/IEC 27551:2021.[18] While standards such as ISO/IEC 27701:2019 are specifically tailored to streamline compliance with legal EU data protection law,[19] the general work of ISO remains a trusted source of inspiration for controllers when rolling-out privacy-specific countermeasures. This is far from an exhaustive list, as the ISO catalogue offers a wide range of generic and sector-specific countermeasures system owners can deploy to address privacy concerns. The GDPR itself acknowledges the importance of standardisation, accreditation and certification, and regulates these approaches in Articles 42 and 43.[20] As such, ISO standards nicely complement the other types of soft-law instruments issued at the EU and national levels and provide controllers with an internationally recognized set of solutions they can implement in their own systems. These documents are designed to address the pacing problem of the law by proposing *ad-hoc* technical countermeasures to specific challenges.[21]

Following a request emanating from the European Commission as per Regulation 1025/2012,[22] the European Committee for Standardization's JTC 13 has recently released standard EN 17529:2022 entitled "Data protection and privacy by design and by default". This long awaited document provides 'requirements for manufacturers and/or service providers to implement Data protection and Privacy by Design and by Default early in their development of their products and services. As such, it constitutes the EU's answer to the growing body of standardisation initiatives undertaken by the ISO.[23]

The standards adopted by the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF), which form the backbone

13 John Borking and others, *Handbook of Privacy and Privacy-Enhancing Technologies - The Case of Intelligent Software Agents* (GW van Blarkom, JJ Borking and JGE Olk eds, College bescherming persoonsgegevens 2003) 3 https://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf.

14 Among the most important fora are the Privacy Enhancing Technologies Symposium (PETS, see: https://petsymposium.org/), the Internet Privacy Engineering Network (IPEN, see: https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network), the International Workshop on Privacy Engineering (IWPE, see: https://iwpe.info/index.html) and the USENIX Conference on Privacy Engineering Practice and Respect (PEPR, see, for the 2023 edition of the conference: https://www.usenix.org/conference/pepr23).

15 George Danezis and others, 'Privacy and data protection by design - from policy to engineering' (European Union Agency for Cybersecurity 2014) 3 http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML.

16 See, for an overview of the most relevant documents: Jean-Pierre Quemard and others, 'Guidance and Gaps Analysis for European Standardisation: Privacy Standards in the Information Security Context' (European Union Agency for Network and Information Security 2018) 11-19 https://data.europa.eu/doi/10.2824/698562.

17 Eric Lachaud, 'The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument' (2018) 34 *Computer Law & Security Review* 244, 251-254. http://www.sciencedirect.com/science/article/pii/S0267364917302121.

18 Preview of these standards can be accessed, respectively, at the following addresses: https://www.iso.org/standard/45270.html; https://www.iso.org/standard/69373.html; https://www.iso.org/standard/71673.html; https://www.iso.org/standard/72018.html.

19 See, for a preview: https://www.iso.org/standard/71670.html. More specifically, Table D.1 provides a one-to-many mapping between all the subclauses of the standard of their corresponding provisions in the GDPR.

20 See, for an overview of the GDPR certification mechanisms ecosystem: Athena Christofi, Pierre Dewitte and Charlotte Ducuing, 'Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020) 147 http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-9489-5.

21 Irene Kamara, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 *European Journal of Law and Technology* 2, 10-11 https://ejlt.org/index.php/ejlt/article/view/545.

22 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, OJ 2012 L 316 12 (ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

23 The European Commission's standardisation mandate indeed dates back from January 2015. See: Commission Implementing Decision on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, accessible here: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2015)102&lang=en.

of all Internet protocols currently in use, have also contributed to shaping online privacy and users' choices. While not pursing any political or value-oriented agenda, these standardization bodies have nonetheless recognised that State or non-State mass surveillance is a "threat against which the Internet engineers should defend" and have therefore integrated privacy among the elements to be taken into account when designing new protocols or updating existing ones.[24] By baking privacy considerations at the core of Internet protocols, Internet standards haven in fact, largely contributed to the very idea of privacy by design.[25]

3. Its progressive integration into the regulatory agenda

As outlined above, the very idea of privacy by design has first manifested itself in the form of punctual technological answers to technological issues, mostly focused on confidentiality. It is only later that the idea of privacy by design started to garner the attention of policymakers, driven by the pervasiveness of privacy-invasive technologies and the ever-complexification of personal data processing infrastructures. In that context, the progressive integration of privacy by design into the regulatory agenda aimed at shaping the way technology is designed by forcing all stakeholders to mitigate its impact on individuals' fundamental rights and freedoms, and influencing early design choices that might prove difficult to revert halfway through the development process.[26] While Article 25(1) GDPR is often perceived as the culmination of these efforts, it is neither the only nor the first manifestation of that approach in a binding legal text.

3.1 The early days

Early traces of privacy by design can be found in various national and EU legislation, if in a more subtle form than what is known today in the GDPR. Deep diving into these initiatives is essential to understand the foundations on which the current EU regulatory framework was built.

3.1.1 National developments

Looking at the United States first, a sketch of that idea can be found in point (e), (10) of the Privacy Act of 1974 that obliges federal agencies to "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity".[27] Section 1173, point (d), (2) of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[28] contains a similar provision, but this time applicable to healthcare providers and extending the goal of the said safeguards to "compliance with [the rules contained in Part C HIPAA]".

One has to wait until 1997 for the term "design" (in this case, "Gestaltung") to make a formal appearance in Article 2, §3, (4) of the German Federal Information and Communication Services Act,[29] where it was used to refer to a particular stage in the development process. "Collecting, processing and using as little or no personal data as possible", specified the now repealed legislation, must prevail when "designing and selecting technical equipment for teleservices". A nearly identical formulation was used in the 2001 revision of the 1990 Federal Data Protection Act,[30] but this time with regard to all systems involving the processing of personal data.[31] While the material scope of both these obligations was limited to designing for data, one could argue they were not throttled by the narrower personal scope of application of their modern counterpart in § 71 of the revised Federal Data Protection Act transposing Article 25 GDPR. By decoupling the obligation to design systems in a certain way from the strict notion of "controller" – contrary to what is done in the GDPR – these provisions broke away from the inherently-flawed premise that controllers are always the ones *actually designing* such systems.

3.1.2 A look at the EU

At the EU level, Article 17(1) and Recital 46 of Directive 95/46 already contained the idea of data protection by design.[32] The former obliged controllers to "implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access", while the latter required them to adopt those measures "both at the time of the design of the processing and at the time of the processing itself". If the wording undeniably recalls that of Article 25(1) GDPR, the goal of the measures to be implemented was narrower, focusing on security.[33]

Article 4(1) of the ePrivacy Directive extends that obligation to providers of publicly available electronic communication services, also emphasising network security.[34] Echoing the German "designing for minimisation" approach, Recital 30 of the ePrivacy Directive also suggests that "systems for the provision of electronic communication networks and services [...] be designed to limit the amount of personal data necessary to a strict minimum". In a similar vein, Recital 46

24 Adamantia Rachovitsa, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue' (2016) 24 *International Journal of Law and Information Technology* 374, 381–382 https://academic.oup.com/ijlit/article-lookup/doi/10.1093/ijlit/eaw012.

25 See, for an overview of the privacy considerations integrated in the developments of Internet standards: Alissa Cooper and others, 'Privacy Considerations for Internet Protocols' (Internet Engineering Task Force 2013) Request for Comments RFC 6973 https://datatracker.ietf.org/doc/rfc6973.

26 See, on that idea: European Data Protection Supervisor (n 7) para 9.

27 Privacy Act of 1974 (https://www.justice.gov/opcl/privacy-act-1974).

28 Health Insurance Portability and Accountability Act of 1996 (https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf).

29 Gesetz Zur Regelung Der Rahmenbedingungen Für Informations- Und Kommunikationsdienste (Informations- Und Kommunikationsdienste-Gesetz - IuKDG) (https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl197s1870.pdf).

30 The 1990 Bundesdatenschutzgesetz has been repealed by Artikel 8 of the Gesetz Zur Anpassung Des Datenschutzrechts an Die Verordnung (EU) 2016/679 Und Zur Umsetzung Der Richtlinie (EU) 2016/680 (https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf). Artikel 1 also contains the revised Federal Data Protection Law following the adoption of the GDPR. A consolidated version of the Federal Data Protection Act in English is available here: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.

31 See § 3a of the 1990 Bundesdatenschutzgesetz as amended in 2001 (https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl101s0904.pdf).

32 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31 (ELI: http://data.europa.eu/eli/dir/1995/46/oj).

33 Aurelia Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*, vol 40 (Springer International Publishing 2018) 84, and more specifically the references mentioned in footnote 86 http://link.springer.com/10.1007/978-3-319-98624-1.

34 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) OJ 2002 L 201/37. Note the use of the *present* tense; indeed, at the time of writing, the ePrivacy Regulation that will eventually replace the ePrivacy Directive is still under negotiation.

introduces the idea of "measures requiring manufacturers of certain types of equipment [...] to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected". Both these Recitals suggest to the imposition of upstream obligations on manufacturers of products and services regardless of their implication in the ensuing processing activities. Doing so would make the implementation of data protection safeguards an integral part of the software engineering process and prevent controllers from invoking the lack of suitable suppliers as a reason for non-compliance with their own obligations. [35] These are, however, but recommendations contained in non-binding texts.

3.2 The awakening

While the above-mentioned initiatives sketched the *idea* of privacy by design, the *term* was only coined in 1998 by Peter-Hope Tindall who used it to describe the process of architecting privacy protection into a system.[36] It gained traction as a legal concept at the beginning of the century with the Workshop on Freedom and Privacy by Design organised as part of the Computers, Freedom & Privacy 2000 conference,[37] as various academics started to push the concept forward.[38] Yet, one has to wait until 2009 for Ann Cavoukian, the then Information and Privacy Commissioner of Ontario, to popularise the concept by building on the earlier work of her office and fleshing out its seven foundational principles.[39] If she was not the first to use that term, she nonetheless played a crucial role in the development of that approach, and her efforts marked a turning point as policymakers on both sides of the Atlantic realised the potential of privacy by design as a flexible tool to regulate complex processing activities.[40]

3.2.1 European case law leading the way

Surprisingly, one can already discern hints of privacy by design in the reasoning developed by both the European Court of Human Rights ("ECtHR") and the Court of Justice of the European Union ("CJEU") in landmark data protection cases way before the adoption of the GDPR. While some might argue that such a retrospective reading of their jurisprudence is a bit far-fetched, the similarities with provisions enacted years later are noticeable enough to warrant a mention.

Starting with *I v. Finland* back in 2008, in which the ECtHR considered that Finland "failed its positive obligation under Article 8 § 1 of the [European] Convention [of Human Rights]" by not ensuring practical and effective protection to exclude any possibility of unauthorised access to information held in a public hospital's patient register".[41] The applicant was treated for HIV in the same hospital she was working at, and complained that the patient register implemented at the time had allowed her colleagues to access her medical record and find out about her illness. She initiated civil proceedings against the entity responsible for the hospital's patient register, but Finnish courts dismissed her claim as she could not prove any actual unlawful access since the register had been designed to only log the identification data of the five most recent consultations. While the ECtHR made no mention of privacy by design in its decision, it nonetheless implied that controllers had to implement the necessary technical measures to ensure the confidentiality of the personal data held in an electronic patient record system as well as the possibility to review the lawfulness of each access to the said data.[42]

The CJEU, on the other hand, is yet to issue a decision dealing *specifically* with the scope of Article 25(1) GDPR.[43] Contrary to the ECtHR in *I v. Finland*, it also hasn't had the opportunity to directly examine the specific impact of a particular design flaw on the fundamental rights to privacy and data protection. Examples often cited in literature rather focused on balancing data protection with one or more competing interests, leading to the prohibition of a certain type of disproportionate privacy-invasive technologies as a whole. This was the case, for instance, for the implementation of filtering systems monitoring electronic communications to block the unauthorised sharing of copyrighted works in *Scarlet Extended*.[44] The same goes for the CJEU's interpretation of the right to erasure with regard to search engines in *Google Spain*, which compelled them to exclude, upon request and after due consideration for the potential public role played by the data subject,

35 European Data Protection Supervisor (n 7) paras 42-43.

36 dataPrivacy Partners Ltd., the company Peter-Hope Tindall founded with his partner Jerrard Gaertner, filed a Canadian trademark application on 19 October 2000 for the word mark "Privacy by Design" based on a claim of use dating back to 4 December 1998. The trademark was granted on 24 February 2003 but expired on 25 July 2019 following the lack of renewal. The details of the trademark application can be accessed here: https://www.ic.gc.ca/app/opic-cipo/trdmrks/srch/viewTrademark/pdf?id=1078687&tab=reg&lang=eng&pdf=1. See, for a reference to Peter-Hope Tindall, footnote 1 in Demetrius Klitou, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design', *Privacy Technologies and Policy* (Springer 2012) 86 https://link.springer.com/chapter/10.1007/978-3-642-54069-1_6.

37 Held on Tuesday 4 April 2000. For the full programme of the Computers, Freedom & Privacy 2000 conference, see: http://www.cfp2000.org/program/full-program.html.

38 Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373 https://scholarship.law.georgetown.edu/facpub/810/; Marc Langheinrich, 'Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems' in Gregory D Abowd, Barry Brumitt and Steven Shafer (eds), *Ubicomp 2001: Ubiquitous Computing* (Springer 2001) http://link.springer.com/10.1007/3-540-45427-6_23. Referenced in footnote 6 of Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International Data Privacy Law* 2 https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipy002/4960902.

39 See, for the 2011 revised version of the 2009 original paper: Ann Cavoukian, 'Privacy by Design - The 7 Foundational Principles' https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. See, for a more thorough presentation of these principles: Ann Cavoukian, Scott Taylor and Martin E Abrams, 'Privacy by Design: Essential for Organizational Accountability and Strong Business Practices' (2010) 3 *Identity in the Information Society* 405 http://link.springer.com/10.1007/s12394-010-0053-z.

40 An excellent summary of the work of her office in the field of privacy by design can be found in the Appendices of Ann Cavoukian, 'Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices' https://collections.ola.org/mon/26012/320221.pdf.

41 *I v. Finland* (2008) paras 47-48 (ECLI:CE:ECHR:2008:0717JUD002051103).

42 Lee A Bygrave, 'Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements' (2017) 1 *Oslo Law Review* 105, 109-111 https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the_.

43 This assertion is backed by the absence of relevant results following detailed queries on the Curia database (accessible here: https://curia.europa.eu/juris/). Exact terms such as "design", "appropriate measures" and "technical measures" were used in combination with references to the relevant EU legislation and with the use of "data protection" as the subject-matter. This is hardly surprising given the ancillary function data protection by design is likely to serve in the reasoning of potentially upcoming CJEU decisions. Lee Bygrave reached the same conclusion back in 2017. See Bygrave (n 42) 111. It is worth noting that cases including Article 25 in their scope are currently pending at the CJEU. See, for instance, C-280/22, C-340/21, C-687/21, C-604/22, C-601/20 and C-807/21.

44 Scarlet extended SA v société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10, [2011] ECR I-11959 (ECLI:EU:C:2011:255), para 50; Belgische vereniging van auteurs, componisten en uitgevers CVBA (SABAM) v netlog NV, Case C-360-10, [2012] electronic Reports of Cases (ECLI:EU:C:2012:85) para 48.

certain items from the list of results presented to end users.[45] In both cases, however, the Court did not extrapolate on the existence of an obligation to consider compliance with data protection law as early as the design stage.

A stronger hint can be found in *Digital Rights Ireland*, in which the CJEU built on the wording of Article 17(1) Directive 95/46 to suggest that ensuring "a particularly high level of protection and security [...] by means of technical and organisational measures" was an integral part of Article 8 of the Charter".[46] In other words, the Court implied that the implementation of such measures is an essential component of the fundamental right to data protection. Barring the temporal aspect inherent to Article 25(1) GDPR, the Court also referred to concepts that the EU legislator would later take inspiration from when drafting the GDPR, such as the cost of implementation.

3.2.2 To the GDPR...

At that time, it had become clear, that Directive 95/46 was in desperate need of a refresh. To prepare the ground for the reform, the European Commission launched a consultation to gather insights on the challenges raised by the emergence of modern technologies and globalisation for data protection. In their joint contribution to the said consultation, the Article 29 Working Party ("WP29") and the Working Party on Police and Justice ("WPPJ") noted that Recital 46 and Article 17(1) "have not been sufficient in ensuring that privacy is embedded in ICT". As such, they argued for the inclusion of a "provision translating the currently punctual requirements into a broader and consistent principle of privacy by design" that is "binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT" [47] While the European Commission largely embraced that approach,[48] the WP29 and WPPJ's suggestion to extend such obligation to both technology designers and controllers did not, however, make it through the legislative process untouched.[49] The EDPS also pushed for,[50] and later welcomed,[51] the introduction of "data protection by design" as a standalone legal requirement in the proposal for a GDPR. Around that time, the WP29 was promoting the role of "privacy impact assessments" ("PIA") as tools to substantiate privacy by design in the field of Radio Frequency Identification ("RFID") applications.[52] In its Opinions, the WP29 insisted on the importance to consider privacy and data protection issues as part of the traditional risk assessment process. Anna Romanou even considered the resulting "Privacy and Data Protection Impact Assessment Framework for RFID Applications"[53] as the landmark European document for privacy by design, as it "examines how privacy could be embedded in RFID tags technology in a positive-sum and win-win way".[54]

The European Commission also exhorted Member States to "encourage network operators to incorporate data protection by design and data protection by default settings" when deploying smart grids and smart metering systems. In line with the position it defended in the proposal for a GDPR, the Commission advocated for that principle to be implemented "at legislative level (through legislation that has to be compliant with data protection laws), at technical level (by setting appropriate requirements in smart grid standards to ensure that infrastructure is fully consistent with the data protection laws) and at organisational level (relating to processing)".[55] It is clear from the above that, towards the end of the reform process, data protection

45 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131-12, [2014] electronic Reports of Cases (ECLI:EU:C:2014:317), paras 80-88.

46 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C-293/12 and C-594-12, [2014] electronic Reports of Cases (ECLI:EU:C:2014:238) paras 66-67. This is deduced from the wording used by the Court when arguing that "Directive 2006/24 does not provide for sufficient safeguards, *as required by Article 8 of the Charter*" (emphasis added). The Court then goes on to detail the reasons for her statement, the first being that "Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers *by means of technical and organisational measures*, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures" (emphasis added). Sharing that opinion, see Lee A Bygrave, 'Article 25 Data Protection by Design and by Default' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 575 https://oxford.universitypressscholarship.com/10.1093/oso/9780198826491.001.0001/isbn-9780198826491-book-part-60.

47 Article 29 Working Party and 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' paras 8, 45, and 46 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf.

48 European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union' 15, and more specifically footnote 30 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

49 Their conception of privacy by design was rather ambitious, as it applied to "hardware and software engineers", with the aim of minimising "difficulties in defining and specifying requirements deriving from the principle of 'privacy by design'". See Article 29 Working Party and Working Party on Police and Justice (n 47) para 51.

50 European Data Protection Supervisor, 'Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy' para 21 https://edps.europa.eu/sites/default/files/publication/10-03-19_trust_information_society_en.pdf; European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A Comprehensive Approach on Personal Data Protection in the European Union"' para 109 https://edps.europa.eu/sites/default/files/publication/11-01-14_personal_data_protection_en.pdf.

51 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Data Reform Package' paras 177-182 https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf.

52 Article 29 Working Party, 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' 5 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp175_en.pdf; Article 29 Working Party, 'Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' 7 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf.

53 Available in the version following the comments provided by the WP29 at the following address: https://digital-strategy.ec.europa.eu/en/library/privacy-and-data-protection-impact-assessment-framework-rfid-applications.

54 Anna Romanou, 'The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise' (2018) 34 Computer Law & Security Review 99, 3 http://linkinghub.elsevier.com/retrieve/pii/S0267364917302054.

55 Recital 11, Articles 3(d), 10-18, 24 of Commission Recommendation of 9 March 2012 on Preparations for the Roll-Out of Smart Metering Systems, OJ 2012 L 73/9 (ELI: http://data.europa.eu/eli/reco/2012/148/oj). Article 5 of the Recommendation required Member States to adopt and apply a data protection impact assessment template that can be found here: https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

by design had imposed itself as one of the cornerstones of the new regulatory framework.

Support for data protection by design did not drop once its integration into the EU legislative acquis was guaranteed. On the contrary. Even after the EU legislator agreed on the final form of Article 25(1), the EDPS continued to flesh out the idea of "privacy conscious engineering" as part of its strategy to "customise existing data protection principles to fit the global digital arena".[56] It also provided EU institutions with a methodology detailing how to take data protection requirements into account throughout the entire life cycle of their IT systems, from early design choices to operation and maintenance.[57] Similarly, it acknowledged that public administrations should lead by example when design ICT solutions and endorsed a call formulated in the 2017 Tallinn Declaration on eGovernment to push data protection by design higher on the Commission's research agenda.[58] The EDPS' prolific work on the topic culminated with a dedicated Opinion summarising the reform process, breaking down the components of Article 25(1) GDPR, and listing the most prominent attempts at operationalising that principle.[59] The European Data Protection Board ("EDPB") quickly followed suit with its own Guidelines mapping the general principles with "key design elements".[60]

3.2.3 ...and beyond

If data protection by design is often associated with the GDPR, it is not its only home in the EU legal order. Its importance was already stressed in the criteria elicited for the interoperability framework to be established under Article 12(3)c of the eIDAS Regulation.[61] Similarly, Article 3(3)e of the Radio Equipment Directive offered the European Commission the possibility to oblige, through delegated acts, manufacturers of certain categories of radio equipment to "incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected".[62] More broadly, the concept percolated through the entire EU data protection law reform and made its way into most of the resulting legislation.[63] Functional – if not always verbatim – equivalents of Article 25(1) GDPR can be found in Article 33 of Regulation 2016/794 setting the rules for Europol,[64] Article 20 of Directive 2016/680 applicable to national law enforcement authorities,[65] Article 67 of Regulation 2017/1939 addressing the European Public Prosecutor's Office,[66] and Articles 27 and 85 of Regulation 2018/1725 dealing with EU institutions, bodies, offices and agencies.[67] The Cybersecurity Act now also includes security by design and by default,[68] granting the ENISA the role of setting up and maintaining a European cybersecurity certification framework for ICT products, services and processes.

More recently, Article 28(1) of the Digital Services Act (hereinafter: "DSA") introduced the obligation for providers of online platforms accessible to minors to "ensure a high level of privacy, safety, and security on their service", even suggesting in Recital 71 that they design "their online interfaces or parts thereof with the highest level of privacy" in mind.[69] Along the same lines, Article 34(1) DSA now requires providers of very large online platforms and of very large online search engines to "diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems", including "any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights [...] to respect for *private and family life* enshrined in Article 7 of the Charter [and] *the protection of personal data* enshrined in Article 8 of the Charter" (emphasis added). Substantiating that risk assessment, Article 35(1) DSA also obliges them to implement "reasonable, proportionate and effective mitigation measures" that can include, among

56 European Data Protection Supervisor, 'Opinion 4/2015 – Towards a New Digital Ethics' 10-11 https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf; European Data Protection Supervisor, 'Opinion 7/2015 – Meeting the Challenges of Big Data' 14-15 https://edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf.

57 European Data Protection Supervisor, 'Guidelines on the Protection of Personal Data in IT Governance and IT Management of EU Institutions' para 41 https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf.

58 All Member States and EFTA countries agreed to take steps, in 2018-2022, to "ensure that information security and privacy needs are taken into consideration when designing public services and public administration information and communication technology (ICT) solutions, following a risk-based approach and using state-of-the-art solutions". The Declaration can be found here: https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration.

59 European Data Protection Supervisor (n 7), more specifically the practical guidance detailed in Section 4.

60 European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

61 Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ 2014 L 257/73 (ELI: http://data.europa.eu/eli/reg/2014/910/oj).

62 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, OJ 2014 L 153/62 (ELI: http://data.europa.eu/eli/dir/2014/53/oj). The European Commission has adopted such delegated act on 29 October 2021.

63 The idea of data protection by design is, however, absent from Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ 2018 L 295/138 (ELI: http://data.europa.eu/eli/reg/2018/1727/oj).

64 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135/53 (ELI: http://data.europa.eu/eli/reg/2016/794/oj).

65 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, OJ 2016 L 119/89 (ELI: http://data.europa.eu/eli/dir/2016/680/oj).

66 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ 2017 L 283/1 (ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

67 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, OJ 2018 L 295/39 (ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

68 See Rec. 12 and 13, Art. 51(1) 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), OJ 2019 L 151/15 (ELI: http://data.europa.eu/eli/reg/2019/881/oj).

69 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ 2022 L 277/1 (ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

others, "adapting the design, features or functioning of their services". In the same vein, the latest compromise amendments proposed by the Parliament to the AI Act include an obligation for "deployers" of high-risk AI systems to carry out a Fundamental Rights Impact Assessment, and list the minimum elements that assessment should include.[70]

The proposal for the long-awaited ePrivacy Regulation does not, however, contain a one-to-one equivalent of Article 25(1) GDPR. Since the latter acts as *lex generalis*, such inclusion would have been redundant.[71] The latest draft nonetheless includes two provisions that directly build on that idea.[72] First, the possibility for end-users, where technically possible, to express their consent through "appropriate technical settings of a software placed on the market permitting electronic communications".[73] Second, the obligation to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risks", as set out in Article 32 GDPR, in cases where information emitted by the terminal equipment of an end-user is collected to enable it to connect to another device based on his or her consent, or for statistical purposes.[74] Whether these provisions will make it through the legislative process untouched is uncertain. Originally scheduled to enter into force at the same time as the GDPR, the Regulation has been stalled for years due to intensive industry lobbying.

As it appears from the above, Article 25(1) GDPR is but the tip of the iceberg; the most visible bit that embodies the *ecology* of data protection by design that now underlies EU data protection law in its entirety. The EU legislator has recently reiterated its commitment to that approach in Chapter V of the European Declaration on Digital Rights and Principles for the Digital Decade, stating that "everyone should have access to digital technologies, products and services that are safe, secure, and privacy-protective by design".[75] In that sense, Article 25(1) GDPR is more than an isolated provision awkwardly slotted in an ambitious Regulation. Rather, it is a transversal legal requirement now deeply rooted in the EU legislative acquis.

3.2.4 Other initiatives

Data protection by design is not confined to the EU, though. In 2010, the International Conference of Data Protection and Privacy Commissioners adopted the Resolution on Privacy by Design in an attempt to encourage awareness-raising activities and stimulate research around that concept.[76] A similar idea made its way into the modernised version of the Convention 108.[77] In a form that is similar to that of Article 25(1) GDPR, Article 10 requires parties to "provide that controllers [...] examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and [...] design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms".

Criticised for its privacy-invasive surveillance programmes and the absence of federal privacy legislation, the United States have, in fact, attempted to pass a legislation obliging entities processing personally identifiable information ("PII") concerning more than five thousand individuals during any consecutive 12-month period to ensure a certain degree of privacy by design. More specifically, Section 103 of the Commercial Privacy Bill of Rights Act of 2011 proposed to oblige the said entities to incorporate "the necessary development processes and practices throughout the product life cycle that are designed to safeguard" the PII at stake, taking into account "the reasonable expectations of such individuals regarding privacy" and "the relevant threats that need to be guarded against in meeting those expectations".[78] Courtesy of Senator John Kerry, the Bill has not made it (yet) into a binding piece of legislation. A similar idea was included in Article 1798.100(e) of the California Consumer Privacy Act of 2018,[79] as amended by the California Privacy Rights Act of 2020,[80] which states that "a business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure".

Hints of privacy by design also transpire from the Federal Trade Commission's ("FTC") settlement in the Google Buzz case.[81] In February 2010, and after limited public beta testing, Google decided to roll out "Buzz", an opt-out social network service tightly integrated in its existing Gmail service. On launch day, Gmail users were presented with the choice to either go straight to their inbox or have a tour of Buzz.[82]

70 See, more specifically, Amendment 413, proposing a new Article 29a: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

71 Recital 5 and Article 1(3) European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 Final - 2017/03 (COD)' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017PC0010.

72 The latest version of the text as discussed by the Council can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN.

73 In its Opinion on the proposal for an ePrivacy Regulation, the EDPS regretted that end-users were only given the *option* to rely on such technical settings, highlighting the inconsistency with Article 25(1) GDPR. Instead, it recommended "an obligation on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices". See European Data Protection Supervisor, 'Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)' 18-19 https://edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf.

74 See Recitals 20a and Article4a(2), and Article 8(2b) of the proposal, respectively.

75 European Commission, European Council and European Parliament, 'European Declaration on Digital Rights and Principles for the Digital Decade' https://ec.europa.eu/newsroom/dae/redirection/document/82703.

76 Resolution on Privacy by Design (http://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf).

77 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 as it will be amended by its Protocol CETS No. 223 (https://rm.coe.int/16808ade9d).

78 Commercial Privacy Bill of Rights Act of 2011 (https://www.congress.gov/bill/112th-congress/senate-bill/799). See, for a more extensive comment on the Commercial Privacy Bill of Rights Act of 2011: David Krebs and Juris Doctor, '"Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law?' (2013) 4 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 1, 10 https://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013-2-krebs.pdf.

79 California Consumer Privacy Act of 2018 (CCPA) (https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5).

80 California Privacy Rights Act of 2018 (CPRA) (https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf). The amendments will only be applicable as of 2023.

81 The press release issued by the FCT as well as all the documents related to the case can be found here: https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz-social-network.

82 For more information on the Google Buzz case, see: Ira S Rubinstein and Nathaniel Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 *Berkeley Technology*

Regardless of their decision, all were enrolled in at least certain features. More worryingly, users who agreed to give the social network a try saw the identity of the individuals they emailed most frequently made public by default including, in some cases, ex-spouses, patients, students, employers or competitors. The privacy backlash that ensued prompted the FTC to initiate a complaint against Google for non-compliance with the terms of its own privacy policy, and deceptive practices when it comes to the enrolment procedure and the provision of inefficient controls.

The FTC eventually settled with Google and obliged the company to implement and maintain a "comprehensive privacy programme" that is "reasonably designed to address privacy risks related to the development and management of new and existing products and services for consumers and protect the privacy and confidentiality of covered information".[83] As noted by Deirdre Mulligan and Jennifer King, these programmes constitute one way for the FTC to compensate for the absence of a dedicated, horizontal privacy by design obligation, and to push companies to bake privacy into their usual production workflow.[84] The FTC compiled its vision in a report proposing a framework for protecting consumer privacy in the 21st century articulated around three components, namely privacy by design, simplified choice for businesses and consumers and greater transparency.[85] Building on its earlier settlement with Google, it hinted at the key role these programmes are likely to play in future enforcement actions. As regretted by Ira Rubinstein when discussing an earlier version of the FTC report, however, the agency has failed to provide detailed guidance to support companies in their privacy assessment process.[86]

Such a concept is, however, nowhere to be found in the Canadian Bill C-11 supposed to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act,[87] the first attempt at modernising the rules contained in the Personal Information Protection and Electronic Documents Act.[88] Further down South, Brazil's Lei General de Proteção de Dados Pessoais ("LGPD") now elevates accountability ("responsabilização e prestação de contas") as one of the general principles underpinning the new data protection regime,[89] paired with the obligation to conduct DPIAs ("relatório de impacto à proteção de dados pessoais") in certain cases[90]. When it comes to security specifically, Article 46(2) of the LGPD goes one step further and even requires controllers to "adopt security, technical and administrative measures to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing as from the conception phase of the product or service until its execution".

4. Its manifestation in the GDPR

The idea underlying the data protection reform was to move away from compliance as a mere ticking-the-box exercise by incentivising controllers to take up a more proactive role in the identification and implementation of appropriate mitigation measures. This required the abolition of the antique, paternalistic obligation for controllers to notify their processing operations to National Supervisory Authorities ("NSAs"), in favour of a more flexible approach articulated around the obligation to maintain a record of processing activities (Article 30 GDPR), to notify data breaches to the competent NSA and the affected data subjects (Articles 33 and 34 GDPR) and to consult the former in cases where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller (Article 36 GDPR).

4.1 The need for a combined reading

In doing so, the GDPR strived to establish a future-proof, technologically neutral framework that responsibilises controllers by shifting the burden of analysing and appropriately mitigating the risks to data subject's rights and freedoms onto them. Known as the risk-based approach, it ensures both the flexibility and scalability needed for the underlying rules to remain pertinent in a wide variety of scenarios. As pointed out by Claudia Quelle, such an approach "provides a way to carry out the shift to accountability that underlies much of the data protection reform, using the notion of risk as a reference point in light of which we can assess whether the organisational and technical measures taken by the controller offer a sufficient level of protection".[91] That risk-based approach is comprised of various pieces scattered across the text of the GDPR. Since these have evolved throughout the reform process, the Annex contrasts the original proposal of the Commission,[92] the version adopted by the Parliament at first reading on 12 March 2014,[93] and the final text as approved by the

Law Journal 1333, 1385-1389 https://heinonline.org/HOL/P?h=hein.journals/berktech28&i=1367.

83 See Order III, point C of the FTC settlement in the Google Buzz case, available here: https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

84 Deirdre K Mulligan and Jennifer King, 'Bridging the Gap Between Privacy and Design' (2012) 14 *Journal of Constitutional Law* 989, 1030 https://scholarship.law.upenn.edu/jcl/vol14/iss4/4. These "comprehensive privacy and security programmes" are included in more recent settlements, including the one concluded with Zoom, SkyMed International and Tapplock. Reference to these examples – and many others – are included in: Federal Trade Commission, 'Federal Trade Commission 2020 Privacy and Data Security Update' https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

85 Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change - Recommendations for Businesses and Policymakers' https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

86 Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26 *Berkeley Technology Law Journal* 1409, 14247 https://www.jstor.org/stable/24118675.

87 Bill C-11 - An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts (https://www.parl.ca/LegisInfo/en/bill/43-2/C-11).

88 Personal Information Protection and Electronic Documents Act (https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html).

89 Art. 6(X) Lei Geral de Proteção de Dados Pessoais (LGPD) (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). An unofficial translation of the LGPD is available here: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation.

90 Artt. 5(XVII) and 38 LGPD.

91 Claudia Quelle, 'Enhancing Compliance Under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 *European Journal of Risk Regulation* 502, 505 http://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/enhancing-compliance-under-the-general-data-protection-regulation-the-risky-upshot-of-the-accountability-and-riskbased-approach/C527DEE76C5E9F7D09830E218D1DCA8D. See also, more specifically, Section III at 508-514.

92 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM/2012/011 Final - 2012/0011 (COD)' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0011%3AFIN.

93 European Parliament, 'Position of the European Parliament Adopted at First Reading on 12 March 2014 with a View to the Adoption of Regulation (EU) No .../2014 of the European Parliament and of the

Council on 8 April 2016.[94]

4.1.1 Article 5(2) – Accountability

The first piece is the recognition of *accountability* as one of the general principles, as proposed by the WP29 early in the reform process.[95] While accountability was originally included among the other principles of Article 5(1) GDPR, the Council decided, in its position at first reading, to move it to a dedicated paragraph. Whether this indicates a willingness to confer it a special, higher status, or merely facilitates the later reference to "paragraph 1" when delimiting the extent of controllers' responsibility, is not apparent from the preparatory works. In any case, the final form of Article 5(2) GDPR reads as follows:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

That principle can be split into two distinct elements. On the one hand, the *responsibility* of controllers to ensure compliance with the principles listed in Article 5(1). On the other, an obligation to *demonstrate* and justify how they did so. In that sense, Article 5(2) only provides a general sense of what accountability entails. As detailed below, other provisions flesh it out.

4.1.2 Article 24(1) – Responsibility

The second is the introduction of a provision detailing the extent of controllers' *responsibilities* when it comes to ensuring compliance with the rules stemming from the Regulation in the form of Article 24(1) GDPR. Here again, its positioning as the first obligation listed under Section 1 of Chapter IV seems to highlight the importance of the shift to an accountability-based regulatory regime. Entitled "responsibility of the controller", Article 24(1) lays down the following:

> "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".

Read in conjunction with Article 5(2), it clarifies the nature of the measures that controllers are expected to implement – i.e., "technical and organisational"–, as well as their objective – i.e., "ensur[ing] that processing is performed in accordance with this Regulation". While the original proposal contained a non-exhaustive list of examples of measures, these were cut in the Parliament's version to only mention "compliance policies and procedures that persistently respect the autonomous choices of data subjects". The final text only included a trimmed down version limited to "appropriate data protection policies". Article 24(1) also lists the elements that controllers must take into account when tailoring the extent of their compliance exercise.[96] Building on an idea originally sketched by the EDPS,[97] the Parliament even suggested that "any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures" implemented. This obligation, however, never made it into the final text.

4.1.3 Article 25(1) and (2) – Data protection by design (and by default)

The third piece is the inclusion of *data protection by design* among the obligations falling on controllers' shoulders. Article 25(1) GDPR reads as follows:

> "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".

The resemblance to Article 24(1) GDPR is striking. The added value of that provision becomes clearer when peeling off its structure, though. While they both list the elements to be taken into account during the risk assessment process and require the implementation of appropriate technical and organisational measures to ensure and demonstrate compliance with the text of the Regulation, Article 25(1) adds a crucial element. That is, the obligation to do so "both at the time of the determination of the means for processing and at the time of the processing itself". As pointed out by the EDPS, Article 25(1) therefore "complements the controller's responsibility laid down in Article 24", "stressing some dimensions of [the measures'] implementation process already implicitly present in Article 24 and adding others, making them all mandatory".[98] That semantic overlap between both provisions confirms their complementarity.[99] Yet, a closer look reveals subtle differences beside the timing aspect. When compared to its shorter sibling, Article 25(1) adds the "state of the art" and the "cost of implementation" to the elements that controllers must factor in their risk assessment process. Besides, the objective of the measures to be

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)' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014AP0212

94 Council of the European Union, 'Position (EU) No 6/2016 of the Council at First Reading with a View to the Adoption of a Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016AG0006%2801%29.

95 Section III.2 Article 29 Working Party, 'Opinion 3/2010 on the Principle of Accountability' https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

96 While the final text of the GDPR integrates this "demonstrability" layer in both Articles 24(1) and 25(1), it is worth noting that the original proposal for a GDPR dedicated it a separate paragraph, even suggesting the intervention of "independent internal or external auditors" to verify the effectiveness of the measures implemented by controllers. These precisions were dropped in the version adopted by the Parliament at first reading.

97 European Data Protection Supervisor (n 51) para 176.

98 European Data Protection Supervisor (n 7) paras 24 and 26, respectively.

99 Lee Bygrave seems to share that interpretation, underlining that Article 25(1) GDPR] "builds on and elaborates the more generally formulated provisions on 'responsibility of the controller' in Article 24". See Bygrave (n 42) 114.

implemented slightly differs.[100] Finally, Article 25(1) also exemplifies the type of measure that controllers can implement – i.e., "such as pseudonymisation" – as well as the principles that must be complied with – i.e., "such as data minimisation".

As reflected in the title of Article 25, data protection by design is often considered together with data protection by default (Article 25(2) GDPR). And for good reasons, as that provision seems to specify rather than complement Article 25(1). At its core, it is but a reaffirmation of both the necessity test that conditions the use of all the lawful grounds listed in Article 6(1) but consent, and of the purpose limitation and data minimisation principles enshrined in Article 5(1)b and c. As pointed out by the ICO, Article 25(2) does not require controllers to resort to a "default to off" solution in situations where certain personal data are objectively necessary to achieve a specific purpose;[101] this would, for the rest, run contrary to the very objective of the necessity test hinted at above. This is especially true when controllers rely on their legitimate interests. Such a reading would require them to have these processing operations "objected to" by default, thereby defeating the entire purpose of Article 6(1)f GDPR. In that sense, Article 25(2) should be read, I argue, as specifying the type of countermeasures that controllers must – in any case – already implement as part of their obligations under Article 25(1) in situations where data subjects are offered a certain degree of agency over the processing of their personal data.

4.1.4 Article 32(1) – Security

The fourth piece is the obligation for controllers and processors to ensure the *security* of their processing operations. Article 32(1) GDPR is formulated as follows:

> "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 [...]".

While the thrust of Article 32(1) is largely similar to that of Article 25(1), it presents two notable differences. On the one hand, a broader personal scope. Compared to Articles 24(1) and 25(1), Article 32(1) indeed obliges both controllers *and* processors to implement the above-mentioned measures. As a result, it does not suffer from one of the main limitations of the former. On the other, a narrower material scope. Indeed, Article 32(1) only substantiates one of the principles outlined in Article 5, namely "integrity and confidentiality". In comparison, Articles 24(1) and 25(1) are transversal requirements designed to give effect to all the general principles listed in Article 5, as well as all the obligations stemming from the text of the Regulation.[102] Including security itself. As such, one could argue that complying with Articles 24(1) and 25(1) already requires controllers to implement appropriate technical and organisational measures to ensure an adequate level of security following the overarching risk-based approach outlined above. This is not to say Article 32 GDPR is redundant, though. Not only does it add processors to the equation, but its second paragraph also provides a non-exhaustive list of risks that must be taken into account when gauging the appropriateness of the measures to be implemented, i.e. "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed".

4.1.5 Article 35(7) – Data protection impact assessments

The final piece is the requirement for controllers to conduct *DPIAs* when certain conditions are met. Beyond their role in the prior consultation procedure outlined in Article 36 GDPR, DPIAs are "important tools for accountability, as they help controllers not only to comply with [the] requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation".[103] Article 35(7) GDPR, which details the minimum content of that assessment, reads as follows:

> "The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

The elements listed in Article 35(7) largely overlap with the steps involved in the risk assessment controllers must *in any case* undertake to comply with Articles 5(2), 24(1), 25(1) and 32(1). In all scenarios, controllers are required to describe their processing activities, identify and mitigate the risks they pose for data subject's rights and freedoms, and ensure a certain degree of accountability for the assessment they performed. As pointed out by Claude Castellucia and his co-authors, a DPIA can therefore be "perceived as part of the 'protection by design and by default' approach".[104] The fact that Articles 5(2), 24(1), 25(1) and 32(1) apply regardless of whether the processing at stake are "likely to result in a high risk to the rights and freedoms of natural persons" suggests that conducting *a* form of DPIA, if not one that strictly follows the requirements imposed by Article 35, is a prerequisite for *all* control-

100 Article 24(1) specifies that the goal of the said measures should be to "to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation", while Article 25(1) mentions measures 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".

101 Information Commissioner's Office, 'Data protection by design and default' (19 May 2023) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/#dpd4 accessed 1 August 2023.

102 Quoting the European Data Protection Supervisor (n 7) para 25 on that point, "[i]t is useful to remind that, whereas the measures identified in Article 32 are just those targeting one of the data protection principles in Article 5, namely the one called "integrity and confidentiality", Article 24 refers to the implementation of all data protection principles and the compliance with the whole of the GDPR".

103 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' 4 https://ec.europa.eu/newsroom/document.cfm?doc_id=47711. "In other words", adds the WP29, "a DPIA is a process for building and demonstrating compliance".

104 Castelluccia and others (n 5) 8, more specifically point 2.2 "Connection with DPIA".

lers. That interpretation is explicitly backed by the WP29,[105] the EDPB[106] and the EDPS,[107] as well as many legal scholars,[108] among whom Bettina Berendt who notes that a "significant part of [data protection by design] is the [DPIA] in which, among other things, the likely impacts of the planned technology on stakeholders' privacy are assessed".[109]

4.1.6 Follow the thread

Summarising all the above, the "by design" narrative of the GDPR goes as follows. Article 5(2) starts by elevating *accountability* as the most prominent of the general principles governing the processing of personal data, requiring controllers to both ensure and demonstrate compliance with the Regulation.[110] Article 24(1) then introduces the *risk* component by substantiating the extent of controllers' obligations as well as outlining the process to get there. Figurehead of the data protection reform, Article 25(1) adds the *timing* dimension, along with additional details on the elements that must be taken into account. Article 32(1) extends the risk-based approach to processors when selecting and implementing the measures necessary to ensure an appropriate level of *security*. Finally, Article 35(7) provides *a* – if not *the only* – way to conduct the *assessment* inherent to the risk-based approach. These provisions are intrinsically linked and should be read together when deciphering the exact scope of data protection by design as a transversal obligation. Claudia Quelle even speaks of the "GDPR's own 'risk triangle'", in which "the data protection impact assessment paves the way towards data protection by design in line with the risk-based responsibility of Art 24(1)".[111]

Understanding the role and added value of data protection by design therefore requires the combined reading of all these provisions. Isolating Article 25(1) from the broader ecosystem in which it operates inevitably leads to the conclusion that Article 25(1) GDPR "is repetitive of other sections of the GDPR and has no identity of its own".[112] While it is true Article 25(1) repeats provisions contained elsewhere in the Regulation, discarding its entire added value based on such overlaps would disregard what they bring to the table *besides* these repetitions. In that sense, data protection by design is *only* about the implementation of measures to ensure compliance with the Regulation, but adds three crucial components. First, the risk-based approach that requires controllers to tailor the extent of their compliance exercise based on a series of variables. Second, the timing aspect that calls for the integration of these considerations as early as possible in the development process and throughout the entire personal data processing life-cycle. And lastly, the accountability layer added by Articles 5(2) and 24(1), which is missing from its counterpart in Article 25(1). While the existence of repetitions is beyond contest, these, I argue, give more meat to an obligation that goes far beyond parroting the remainder of the Regulation. As such, data protection by design acts as an overarching obligation that requires controller to ensure and demonstrate compliance with *all the provisions of the Regulation* by following a *risk-based approach*, and doing so *throughout the whole data processing life-cycle*.

4.2 The role of data protection by design in the GDPR

Beside its role as a standalone obligation, data protection by design also acts as a reference point for other provisions in the GDPR, and therefore serves a broader purpose than "merely" obliging controllers to implement appropriate technical and organisational measures.

4.2.1 A ground and a yardstick for fines

As is the case for all the principles and obligations contained in the Regulation, NSAs can assess compliance with Article 25(1) when exercising the powers laid down in Article 58.[113] More specifically, Article 58(2)i paves the way for the imposition of administrative fines pursuant to Article 83 in addition to, or instead of, the other corrective measures listed in that paragraph. Article 25(1) GDPR plays a double role in that context.

First, any infringement of that provision can lead to the imposition of an administrative fine up to 10 000 000 EUR or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4)a GDPR). That such a core principle of the Regulation falls in the lower tier of sanctionable conducts may seem surprising. This deserves to be nuanced, though. First off, even that lower threshold far exceeds the enforcement powers granted to supervisory authorities under Directive 95/46. Plus, as explained in Section 4.1, Article 25(1) is but one piece of the broader accountability narrative, and should be read in conjunction with Articles 5(2), 24(1), 32(1) and 35. As a result, a breach of Article 25(1) will *often* go hand in hand with a breach of accountability, which itself falls in the higher tier pursuant to Article 83(5)a.[114] For instance, the Polish authority relied on Article 5(2) alongside Article 25(1) to fine Virgin Mobile Polska 1,968,524 PLN (approximately 460,000 EUR) for the lack of appropriate security measures, including regular testing and evaluation, leading to a personal data breach affecting 114,963 custom-

105 Article 29 Working Party (n 103) 6, which underlines that "[t]he mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects".

106 European Data Protection Board (n 60) para 32, which clarifies that "controllers [...] must *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" (emphasis added).

107 European Data Protection Supervisor (n 7), stating that "Article 35 provides for a mandatory [...] DPIA when the processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. This *complements* the mandatory risk management approach of Article 24 when the organisation estimates that the level of risk for the individuals whose data are processed is high. The DPIA represents an outstanding accountability tool and organisations may benefit from adopting this approach *also in cases where it is not mandatory*" (emphasis added).

108 See, among others, Giorgia Bincoletto (n 2) 172; Lina Jasmontaite and others, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4 European Data Protection Law Review 168, 173 https://edpl.lexxion.eu/article/EDPL/2018/2/7; Bygrave (n 42) 115; Inga Kroener and David Wright, 'A Strategy for Operationalizing Privacy by Design' (2014) 30 The Information Society 355, 360 https://doi.org/10.1080/01972243.2014.944730; Danezis and others (n 15) 11-12.

109 Bettina Berendt, 'Better Data Protection by Design Through Multicriteria Decision Making: On False Tradeoffs Between Privacy and Utility', *Privacy Technologies and Policy* (Springer International Publishing 2017) 211 https://link.springer.com/chapter/10.1007/978-3-319-67280-9_12.

110 The EDPB seems to share that interpretation. See European Data Protection Board (n 60) para 64, which highlights that "[t]he accountability principle is *overarching*: it requires the controller to be responsible choosing the necessary technical and organisational measures" (emphasis added).

111 Quelle (n 91) 505. "The risk-based approach", she adds, therefore "provides a way to carry out the shift to accountability that underlies much of the data protection reform".

112 As such, he adds, the measures to be implemented pursuant to Article 25 "reflect requirements embodied in other sections of the GDPR". See: Waldman (n 3) 153, 157.

113 European Data Protection Board (n 60) paras 92-93.

114 Compared to the lower tier of infringements listed in Article 83(4) GDPR, these can be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

ers.[115] Other provisions might also come into play, as a breach of data protection by design will *almost inevitably* involve an infringement of the principles and obligations for which the controller has failed to implement appropriate technical and organisational measures. In its decision against the Italian telecom operator Fastweb, for example, the Italian regulator considered the failure to control the data acquisition chain to exclude unlawful promotional calls as a breach of Articles 5(1), 5(2), 6(1), 7, 24, and 25(1) GDPR.[116] These principles and obligation are also subject to the higher threshold of Article 83(5). In other words, since NSAs are unlikely to issue administrative fines based on a breach of Article 25(1) *alone*, they are equally unlikely to be limited by Article 83(4).

When calculating the amount of a fine for a breach of data protection by design, NSAs tend to consider a given set of linked processing operations as a *single* sanctionable conduct that gives rise to *multiple* infringements, including but not limited to Article 25(1).[117] In the absence of concurrence of offences,[118] the "unity of processing" rule of Article 83(3) GDPR comes into play to ensure that "the total amount of the administrative fine [does] not exceed the amount specified for the gravest infringement". Recent decisions have applied that reasoning. The Finnish authority, for instance, considered the requirement imposed on data subjects to send a filled and signed paper form to exercise their right to erasure, the failure to answer access request and the absence of beta testing for its email system – that last negligence being the breach of Article 25(1) GDPR – as *one* sanctionable conduct leading to *multiple* infringements for which a *single* fine was imposed pursuant to Article 83(3) GDPR.[119] Similarly, the Hungarian authority hit Budapest Bank with a *single* 700,000 EUR fine based on *multiple* infringements, including Articles 24(1) and 25(1), for failure to conduct and document the necessity and proportionality assessments prior to the rolling-out of an AI-based voice analysis software used by customer services, and the lack of transparency vis-à-vis data subjects.[120] The Hungarian authority therefore calculated the amount of the fine based on Article 83(5), rather than Article 83(4).[121]

In these cases, Article 25(1) almost acted as an *aggravating circumstance* to underline the fact that the controller had failed to implement the necessary measures to comply with *another* provision *by design*. The risk is, of course, to see NSAs automatically include Article 25(1) in the list of infringements since, in theory, compliance with *any* provision would require the implementation of *at least some* appropriate technical and organisational measures to that end. Right now, supervisory authorities seem to throw Article 25(1) among the list of infringements for any kind of sanctionable conduct regardless of whether the controller has failed to comply with the characteristics that make data protection by design *different* from a mere repetition of the provisions it aims to ensure compliance with, namely, as discussed above, the risk-based approach and the timing aspect. Meaningful enforcement of Article 25(1), I argue, would require NSAs to justify the *reasons why* the controller has failed to substantiate these two elements in a given scenario. In that sense, the default inclusion of that provision in every single decision is of limited added-value.

This is not to say that NSAs will never issue a fine based *exclusively* on non-compliance with Article 25(1). But the probability seems rather low as this would sanction the lack of an *overall* process to substantiate the risk-based approach and, therefore, require NSAs to include the majority – if not all – the processing operations undertaken by the controller within the scope of their decision. The recent decision issued by the Irish authority against Meta Platform Ireland Limited for its implementation of Facebook's and Instagram's contact matching feature is a case in point. While the 265,000,000 EUR fine is based *exclusively* on a breach of Article 25(1), the entire reasoning is articulated around the failure to implement appropriate technical and organisational measures in respect of the *purpose limitation* and *integrity and confidentiality* principles.[122] When investigating on their own initiative, NSAs could therefore, at least in theory, identify *two sanctionable conducts* leading to *two separate fines*; one for non-compliance with Article 25(1), and another for one or more specific infringements.[123] To the best of my knowledge, however, this has not happened yet. Such a scenario is even less likely to arise when following up on complaints, as data subjects are often required to *precisely* delineate the processing activities they consider in breach of the Regulation, as well as *all* the alleged infringements. Here again, it is fairly unlikely that they would target all the controller's processing operations to only pinpoint a single infringement. Besides, a decision based on Article 25(1) GDPR *alone* would not contribute much to clarifying the scope of a provision that, some say, is too vague to be meaningfully enforced.[124]

115 Prezes Urzędu Ochrony Danych Osobowych, Decyzja DKN.5112.1.2020, 17-18 https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020. More specifically, the Polish supervisory authority held that "the Company did not properly implement the requirements of Regulation 2016/679 to the extent set out in Article 24(1), Article 25(1), Article 32(1)(b) and (d) and Article 32(2) of Regulation 2016/679".

116 Garante per la protezione dei dati personali, Provvedimento del 21 luglio 2022 [9808698], point 2.2.1, pp. 15-18 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9808698). The Garante held a similar reasoning when fining, respectively, the telecom operators Wind Tre 16,729,600 EUR in decision 9435753 (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435753), and TIM 27,802,946 EUR in decision 9256486 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486).

117 See the reasoning and diagram presented in Chapter 3: "Concurrent infringements and the application of Article 83(3) GDPR", and in point 3.1.2 more specifically, of European Data Protection Board, 'Guidelines 04/2022 on the Calculation of Administrative Fines Under the GDPR' paras 21-46 https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

118 That is, "where one provision is neither precluded nor subsumed by the applicability of the other, because they do not fall in scope of the principles of specialty, subsidiarity or consumption and mostly pursue different objectives" as detailed in European Data Protection Board (n 117) paras 30-37.

119 Tietosuojavaltuutetun toimisto, Decision 6097/161/21 against Otavamedia Oy, 33-40 (https://finlex.fi/fi/viranomaiset/tsv/2022/20221483). As summarised at the beginning of the Decision of the Sanction Committee, the fine was issued for infringement of Articles 25(1), 12(1), (2), (3) and (4), 15 and 17 GDPR.

120 Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision NAIH-85-3/2022 against Budapest Bank, para 104 (https://naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei). More specifically, "the customer's data management practices in relation to the automated analysis of customer service voice recordings [...] violate Article 12(1), Article 24(1), Article 25(1) and (2)".

121 Decision NAIH-85-3/2022 (n 120), para 53.

122 Data Protection Commission, Decision IN-21-4-2 against Meta Platforms Ireland Ltd., paras 167-169 (https://www.dataprotection.ie/sites/default/files/uploads/2022-12/Final%20Decision_IN-21-4-2_Redacted.pdf).

123 European Data Protection Board (n 117) under "Multiple sanctionable conducts" paras 45-46.

124 See, for instance, 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' (2020) 10 International Data Privacy Law 37, 55 http://academic.oup.com/idpl/article/10/1/37/5607285, arguing that "imposing large fines on companies that violate Article 25 would seem improper given the lack of clarity over what Article 25 requires or how it relates to other more substantive provisions"; Bygrave (n 42) 117, noting that "[i]nvoking stiff sanctions for breach of Article 25(1) will not be easy given the very general

Second, the degree of compliance with Article 25(1) GDPR serves as a yardstick to determine the amount of a potential fine. Articles 83(2)d indeed requires NSAs to consider, among other elements, "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". This is mostly relevant when multiple actors are involved in the processing since, as the CJEU likes to recall, "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data".[125] This is then combined with an assessment as to the appropriateness of the measures referred to in Articles 25 and 32, for which NSAs will have to evaluate "the extent to which the controller 'did what it could be expected to do'".[126] Considered together, Articles 83(2)d, 84(4) and 84(5) therefore create infinite variations of responsibilities that can modulate the corresponding fine.

4.2.2 A consideration for public tenders

During the reform process, the European Parliament suggested the addition of an extra paragraph to make data protection by design a "prerequisite for public procurement tenders according to Directive 2004/18/EC [and] Directive 2004/17/EC [now both repealed, NDLR]".[127] The Council decided to delete that paragraph and replace it with a watered-down version in the form of Recital 78 that now suggests that "the principles of data protection by design [...] be taken into consideration in the context of public tenders". This is far less constraining for contracting authorities as Recitals are not binding but simply orient the interpretation of the main provisions. While tenderers are likely to qualify as either controllers or processors down the line, and will therefore have to comply with Articles 25(1) and 32 *anyway*, building on the Parliament's suggestion would have systematised the inclusion of robust data protection safeguards in tender specifications.

4.2.3 A criterion for data breach notifications

The type of measures implemented also plays a role in assessing whether controllers must communicate personal data breaches to the affected data subjects. Article 34(1) GDPR requires them to do so "[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons". However, paragraph 3 relaxes that obligation in cases where "the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption". Technical measures "effectively limiting the likelihood of identity fraud or other forms of misuse", adds Recital 88 GDPR, should also be taken into consideration when determining whether a controller should communicate such a breach.

4.2.4 An element of the compatibility assessment

Lastly, the existence of appropriate safeguards also influences the outcome of the compatibility assessment that is required when personal data are processed for a different purpose than that for which they have been collected (Article 6(4)e GDPR). If this is now explicitly acknowledged in the Regulation, it builds on a criterion that Article 6(1)b of Directive 95/46 already hinted at back in 1995, if only for further processing for historical, statistical or scientific purposes.[128] In its opinion on purpose limitation, the WP29 nonetheless derived a general principle out of that narrow provision, noting that "appropriate additional measures could [...], in principle, serve as 'compensation' for a change of purpose" in general.[129] This, it added, "might require [the implementation of] technical and organisational measures", having regard to "certain basic goals of data protection and data security" such as "availability, integrity and confidentiality", and "transparency, isolation and 'intervenability'". The WP29 provided examples of what would constitute "relevant measures", referring to "full or partial anonymisation, pseudonymisation, or aggregation of the data, privacy enhancing technologies, as well as other measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation')". All of which are now part of the "by design" narrative.

5. Conclusion

This paper traced back the origins of data protection by design, starting with its early inception in the software engineering community all the way up to its integration as a dedicated provision in the GDPR. In doing so, it also painted a broad picture of all the initiatives that have preceded the Regulation both within and outside the EU. Eventually, that retrospective led the conclusion that, more than an extra obligation, Article 25(1) GDPR embodies the broader shift to a risk-based approach that not only percolates through the text of the GDPR itself, but also transpires from many other regulatory frameworks that seek to shield individuals from the harmful consequences of privacy-invasive technologies. Ari Waldman criticises Article 25(1) GDPR for not being "a faithful reflection of the privacy by design literature".[130] While I agree with that observation, I consider that a feature, rather than a bug. Instead of merely transposing a pre-established conception of "privacy by design" that would have inherited years of controversies, the EU legislator took inspiration from the rich historical background behind that concept, and came up with its *own* codification in the form of Article 25(1) GDPR. This is a sui generis concept that bears a specific meaning within the context of the Regulation.

That flexible approach, articulated around the "appropriateness" of the measures to be implemented by the actors concerned, is essential to ensure that the principles and rules enacted to combat these issues remain relevant despite the constant evolution of processing

(and process-oriented) way in which its obligations are formulated".

125 See, on that note, Unabhängiges landeszentrum für datenschutz schleswig-holstein v wirtschaftsakademie schleswig-holstein GmbH, Case C-210/16, [2018] electronic Reports of Cases (ECLI:EU:C:2018:388) para 43; Tietosuojavaltuutettu, Case C-25/17, [2018] electronic Reports of Cases (ECLI:EU:C:2018:551) para 66; Fashion ID GmbH & coKG v verbraucherzentrale NRW eV, Case C-40/17, [2019] electronic Reports of Cases (ECLI:EU:C:2019:629) para 70.

126 Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679' 13 https://ec.europa.eu/newsroom/article29/redirection/document/80836.

127 European Parliament (n 92), Article 23(1a), Amendment 118. The reason for its inclusion in the text of the Regulation are not detailed in the Parliament's report accompanying its position at first reading, though.

128 Article 6(1)b Directive 95/46 specified that "[...] personal data must be: collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards".

129 Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' 26-27 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. See, more specifically, footnote 75 that broadens the role of such appropriate safeguards beyond further processing for historical, statistical or scientific purposes, noting that "[t]his follows *implicitly*" from Article 6(1)b of Directive 95/46 (emphasis added).

130 Waldman (n 3) 158.

technologies. This gives NSAs the upper hand when it comes to orienting controllers' practices, either by issuing *ad-hoc* guidance, or through administrative remedies as part of their investigation and corrective powers. That governance structure, however, hinges upon the proper functioning of the coope ration and consistency mechanism put in place by Article 60 GDPR,[131] and on the allocation of sufficient resources to NSAs.[132]

Understanding the genesis of Article 25(1) GDPR is an essential prerequisite to properly grasp its role and implications for controllers. As the first part of a two paper series, this first paper laid the groundwork for a deeper analysis of its material and personal scope of application. Indeed, the former does not clearly appear from a literal reading of that provision, while the latter has crystallised many criticisms as it only covers controllers,[133] rather than the entities actually in charge of the design of the system. Against that background, that second paper will shed light on both these aspects by breaking down the components of data protection by design as materialised in Article 25(1) GDPR, namely (i) the implementation of appropriate measures to ensure and demonstrate compliance with the provisions of the Regulation, (ii) the risk-based approach articulated around 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 and (iii) the timing aspect, which requires controllers to act upon Article 25(1) both at the time of the determination of the means for processing and at the time of the processing itself. That analysis will be supported by an extensive case law review spanning multiple EU countries in an attempt to dissect how these notions have been interpreted by NSAs since the entry into force of the Regulation. The legal-historical overview proposed in this paper will serve as reference point when analysing these decisions.

Annex. The 'by design' approach throughout the reform process

See table in annex.

The table details the evolution of Articles 5(2), 24 and 25(1) and (3) GDPR throughout the legislative process that led to the adoption of the GDPR. The texts used for the analysis are, respectively, the proposal issued by the European Commission,[134] the position of the European Parliament adopted at first reading on 12 March 2014,[135] and the position of the Council adopted at first reading on 8 April 2016.[136] That last version corresponds to text approved by the European Parliament and the Council on 27 April 2016. Each row provides a snapshot of a certain aspect at a given point in time.

The table uses colours to denote the type of modification, using the definitive version of the Regulation as a reference point. Passages in red have been cut from the final text. Those written in orange have made it through the trialogue, but in a slightly different form. In these cases, the modified version corresponds to the orange text in the "Council" column. Those written in green represent additions brought by the Council that were neither included in the original proposal, nor mentioned in the Parliament's position at first reading. Lastly, those written in blue have been kept, but moved to a different provision. Here again, the blue text under the "Council" column shows where the said passage has been integrated.

131 Amidst criticisms around the bottleneck role attributed to the Irish regulator, the European Commission has recently announced, following a recommendation from the European Ombudsman (available here: https://www.ombudsman.europa.eu/en/decision/en/164337), that it would soon start monitoring large-scale cross border enforcement investigations under the GDPR. See here: https://www.iccl.ie/wp-content/uploads/2023/01/FOLLOW_UP_202200097_20230124_122005.pdf.

132 For an overview of NSAs' resources, see: European Data Protection Board, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf.

133 Ira S Rubinstein and Nathaniel Good (n 124) 43; Lee A Bygrave (n 42) 118; Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law & Security Review 509, 517; Demetrius Klitou, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design', *Privacy Technologies and Policy* (Springer 2012) 93-93 https://link.springer.com/chapter/10.1007/978-3-642-54069-1_6; Sarah Spiekermann, 'The Challenges of Privacy by Design' (2012) 55 Communications of the ACM 38, 40 https://dl.acm.org/doi/10.1145/2209249.2209263.

134 European Commission (n 91).

135 European Parliament (n 92).

136 Council of the European Union (n 93).