Technology and Regulation

The Many Shades of Impact Assessments

An analysis of data protection by design in the case law of national supervisory authorities

Author(s)	Pierre Dewitte
Contact	pierre.dewitte@kuleuven.be
Affiliation(s)	KU Leuven Centre for IT & IP Law - imec

Keywords	GDPR, Accountability, Responsibility, Data protection by design, Case law review, Decisions repository		
Published	**Received**: 30 Apr. 2024	**Accepted**: 3 Jul. 2024	**Published**: 11 Sep. 2024
Citation	Pierre Dewitte, Dionysios Pelekis, The Many Shades of Impact Assessments, Technology and Regulation, 2024, 209-253 • https://doi.org/10.26116/techreg.2024.018 • ISSN: 2666-139X		

Abstract

Data protection by design is one of the cornerstones of the reform that led to the adoption of the GDPR. Yet, the very nature of that obligation, coupled with the broad wording used by the EU legislator, makes substantiating data protection by design particularly complex. This paper is the second part a two-paper series that explores the intricacies of Article 25(1) GDPR. While the first entry delved into the history and role of data protection by design, this paper aims to clarify the material scope of that provision. It does so by analysing the three core components of Article 25(1) GDPR in light of the findings of a case law review spanning 177 administrative and judicial decisions issued by 26 supervisory authorities in 24 countries between the entry into force of the GDPR and 31 December 2023. That process exposed the role of data protection by design as a proxy to Fundamental Rights Impact Assessments and shed light on its added value in guaranteeing the flexibility and future-proofness of the Regulation.

1. Introduction

Data protection by design is one of the cornerstones of the reform process that led to the adoption of the General Data Protection Regulation ("GDPR") back in 2016. The whole idea behind Article 25(1) GDPR was to move away from compliance as a mere ticking-the-box exercise–or "window dressing"–by incentivising controllers to take up a more proactive role in the identification and implementation of appropriate mitigation measures.[1] In other words, by setting an overall objective while granting regulatees a certain

1 European Data Protection Supervisor, 'Opinion 5/2018 - Preliminary Opinion on Privacy by Design' (2018) para 13 <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 28 April 2023, noting that "in the past, privacy and data protection have been perceived by many organisations as an issue mainly related to legal compliance, often confined to the mere formal process of issuing long privacy policies covering any potential eventuality and reacting to incidents in order to minimise the damage to their own interests".

discretion as to how to actually get there. Yet, the very nature of that obligation, coupled with the broad wording used by the EU legislator, makes substantiating data protection by design a particularly precarious endeavour. This paper is the second part of a two-paper series that seeks to unravel the material scope of data protection by design understood within the meaning of Article 25(1) GDPR. The first entry of the series, entitled "A Brief History of Data Protection by Design: From multilateral security to Article 25(1) GDPR" ("the first paper"), traced back the history of that concept starting with its early inception in the software engineering community up to its integration as a dedicated provision in the Regulation. It also argued for the combined reading of Articles 5(2), 24(1), 25(1) and 35(1) when interpreting that concept.[2] These provisions are therefore interchangeably used to support the reasoning deployed in this paper. I therefore invite the reader to briefly go through that first publication, as it sets the scene for many of the points discussed here. I also encourage them to consider the finding of a comparable initiative conducted by Christina Michelakaki and Sebastião Barros Vale back in 2023.[3]

The history and role of data protection now clarified, the objective of this paper is to delineate the exact scope of controllers' obligations under Article 25(1) GDPR by dissecting each of that provision's constitutive elements in an attempt to (i) identify the type of measures that controllers must implement, (ii) clarify the nature of the risk assessment exercise they must conduct, and (iii) understand the implications of the oh-so crucial timing aspect. It does so by stitching together the hints scattered in legislation, non-binding European and national soft law instruments such as guidelines and opinions and, most importantly, the jurisprudence issued by National Supervisory Authorities ("NSAs") on the matter. More specifically, it analyses each of these components in light of the findings of a case law review spanning 177 administrative and judicial decisions issued by 26 NSAs in 24 countries between the entry into force of the GDPR and 31 December 2023. Given the scope of the case law review, this paper only discusses a selection of the most relevant teachings gleaned from the reading. The raw materials that served as the basis for that exercise, as well as all the findings, including those that did not warrant an explicit reference in this piece, are available as supplementary materials to the present contribution in the form of a downloadable archive.[4] That archive is designed as an offline resource and contains the metadata of all 177 decisions, their full text in both original and translated version, as well the output of the review process structured around the three components of data protection by design.

Important remark. The methodology, content and form of the case law review are detailed in the README.txt file included as part of the supplementary materials. The said file is formatted in Markdown, and can be visualised using any Markdown editor such as MarkText or StackEdit. Besides, and to avoid footnotes overload, this paper derogates to the OSCOLA style when referencing the decisions that are included in the case law review. Instead of the traditional footnote, these cases are referenced in the main text using their name or reference number as specified in column "A" of the Excel sheet entitled "Decisions repository" contained at the root of the archive file, together with, an embedded URL to their original source. All the other bibliographical information, including the exact administrative or judicial authority that issued the decision, its date and the identity of the parties involved can be found in the corresponding columns of the said "Decisions repository".

Before delving into each individual component, it is worth noting, as did the EDPS, that the "processing of personal data, partially or completely supported by IT systems, should always be the outcome of a *design project*" (emphasis in original).[5] Just like any other "project" *stricto sensu*,[6] it therefore requires careful planning, continuous support, as well as concerted efforts to get right. This might seem obvious, but nonetheless carries the idea that the existence of *a* process is more important than the exact steps involved, as long as it is designed to achieve a well-defined purpose. In this case, compliance with the principles

2 Pierre Dewitte, 'A Brief History of Data Protection by Design: From Multilateral Security to Article 25(1) GDPR' [2023] Technology and Regulation 80 <https://techreg.org/article/view/13807> accessed 10 January 2023.

3 Christina Michelakaki and Sebastião Barros Vale, 'Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR' (Future of Privacy Forum 2023) Report <https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf> accessed 7 Janaury 2024.

4 The supplementary materials are hosted on KU Leuven RDR, and accessible here: <https://doi.org/10.48804/23MRLG> accessed 10 January 2023.

5 European Data Protection Supervisor (n 1) para 27.

6 That is, "a task requiring considerable or concerted effort", Collins Concise English Dictionary (HarperCollins Publishers 2011) <https://www.collinsdictionary.com/dictionary/english/effort> accessed 10 January 2024.

and rules of the GDPR. While the open-ended wording of Article 25(1) fuels a lively debate as to its precise material scope, that flexibility is the keystone of the risk-based approach, and the one characteristic that makes it an innovative approach to regulation. One should also keep in mind, as recently highlighted by the CJEU in Case C-340/21, that "the terms of a provision of EU law, such as Articles 24 and 32 of the GDPR, which makes no express reference to the law of the Member States for the purposes of determining its meaning and scope must normally be given an *autonomous* and *uniform* interpretation throughout the European Union, having regard, *inter alia*, to the wording of the provision concerned, to the objectives pursued by that provision and to its context" (emphasis added).[7]

The goal of this paper is to propose a documented take on the scope and role of the three core components of data protection by design, namely (i) the implementation of appropriate technical and organisational measures, (ii) the risk-based approach to compliance, and (iii) the continuous nature of that exercise. To do so, Section 2 first delves into the type of measures that controllers are expected to implement pursuant to Article 25(1) GDPR. In doing so, it sheds light on the threshold for "appropriateness", assesses the impact of the requirements for these measures to be of "technical and organisational" nature, and calibrates the material scope of data protection by design in light of the broader objective pursued by the Regulation. Next, Section 3 examines the substance and role of each of the criteria listed in Article 25(1), namely the "state of the art", the "cost of implementation", the "nature, scope, context and purposes" of the processing as well as the "risks of varying likelihood and severity for the rights and freedoms of natural persons" raised by that processing; that last criterion being the *pièce de résistance*. Lastly, Section 4 explores the temporal scope of data protection by design, and outlines the challenges it poses in the current software production and implementation dynamic. Section 5 then outlines the key takeaways from the case law review.

2. The implementation of measures

First and foremost, complying with Article 25(1) GDPR requires the implementation of some sort of *measures*. This is the essence of data protection by design, and the ultimate objective any methodology developed to substantiate that principle should aim for. In that sense, the risk-based approach and the timing aspect are but modalities structuring the process leading to their identification and deployment.

2.1 Appropriate measures

The GDPR is light on details when it comes to the *actual* measures controllers have to implement in order to comply with data protection by design. The only apparent precision being that they must be "appropriate". This is a recurring critique among legal scholars,[8] some of whom claim the vagueness and complexity of Article 25(1) "impedes the 'regulatory conversation' between not just EU legislators and other members of the legal community but, more crucially, between EU legislators and data protection authorities on the one side and, on the other side, the community of persons who actually work at the 'coalface' of information systems development".[9] 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

7 *VB v Natsionalna agentsia za prihodite*, Case C-340/21 [2023] electronic Reports of Cases (ECLI:EU:C:2023:986) para 23.

8 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) 168 <http://link.springer.com/10.1007/978-3-030-21752-5_11> accessed 14 January 2024; Seda Gurses, Carmela Troncoso and Claudia Diaz, 'Engineering Privacy by Design' (2011) Unpublished 1, 2 <https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf> accessed 14 January 2024; 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> accessed 14 January 2024; 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 <http://www.script-ed.org/?p=406> accessed 14 January 2024.

9 Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 1 *Oslo Law Review* 105, 117 <https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the_> accessed 17 January 2024.

design as a "catch-all provision that has no identity of its own".[10] The following paragraphs aim at gauging whether these critiques are founded and, should that be the case, whether the generic nature of that provision constitutes an insurmountable roadblock to its proper implementation.

2.1.1 Measures

As rightly pointed out by Dag Wiese Schartum, the Regulation does not define the notion of "measure" in Article 4 alongside the other core concepts used throughout the text, despite being a staple in many provisions.[11] Yet, the GDPR does provide some examples of measures controllers can put in place to comply with data protection by design. Article 24(2) suggests "the implementation of appropriate data protection policies", while Article 25(1) refers to "pseudonymisation". Recital 78 adds in measures that consist in "minimising the processing of personal data, pseudonymising personal data as soon as possible, [ensuring] transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing [and] enabling the controller to create and improve security features''. Article 32(1) also provides a non-exhaustive list, among which "pseudonymisation", "encryption", "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services", "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident" and "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".

The vast soft law apparatus orbiting around the GDPR partially fills the gaps left by the Regulation. In an attempt to clarify the notion of "technical and organisational measures", the EDPB stated that these could be "anything from the use of advanced technical solutions to the basic training of personnel", and provided many examples among which–once again–pseudonymisation.[12] More interestingly though, it also paired each of the general principles of Article 5 GDPR with "key elements" that, while neither exhaustive nor binding, serve as valuable sources of inspiration for controllers when reflecting on the properties of the corresponding measures.[13] More recently, and in the context of its tasks under the Cybersecurity Act, ENISA has also looked at how specific technologies can help controllers comply with specific data protection principles in the context of various personal data sharing scenarios, including in the health sector and when using third party services such as data intermediaries and digital clearinghouses.

NSAs have also issued useful guidance on the matter. As part of its "Privacy Impact Assessment Guidelines", the French Commission Nationale de l'Informatique et des Libertés ("CNIL") has, for instance, published a catalogue of controls aimed at complying with the Regulation and treating the risks posed by the processing of personal data.[14] Similarly, the Agencia Española de Protección de Datos ("AEPD") has compiled a list of

10 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> accessed 17 January 2024. In his conclusion, he argues that "only a robust teleological interpretation can rescue Article 25(1) from its purgatory".

11 Short of such a definition, he assumes that "legislators have applied this term in accordance with a common meaning of the word". See: Dag Wiese Schartum, '"Technical and Organisational Measures" – A Systematic Analysis of Required Data Protection Measures in the GDPR' in Jean Herveg (ed), *Deep Diving into Data Protection*, vol 2021 (1st edn, Larcier 2021) 291 <https://www.larcier.com/fr/deep-diving-into-data-protection-2021-9782807926493.html> accessed 18 January 2024.

12 See European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' para 9 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 18 January 2024. The EDPB refers to the use of "structured, commonly machine-readable format", the possibility for data subjects to "intervene in the processing", the provision of information "about the storage of personal data", the deployment of "malware detection systems"; the "training [of] employees about basic 'cyber hygiene'", the establishment of "privacy and information security management systems" and even the act of contractually obliging processors "to implement specific data minimisation practices".

13 European Data Protection Board, 'Guidelines 4/2019' (n 12) paras 60–88.

14 Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) 3: Knowledge Bases' <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 18 January 2024; See also, for an open source, collaborative guide aimed specifically at software developers: Commission Nationale de l'Informatique et des Libertés, 'GDPR Developer's Guide'<https://github.com/LINCnil/GDPR-Developer-Guide> accessed 18 January 2024; Complementing the above, the Laboratoire d'Innovation Numérique de la CNIL ("LINC") has set up a website to provide concrete, practical examples of measures designed to implement key GDPR concepts. See: Laboratoire d'Innovation Numérique de la CNIL, 'Données & Design' <https://design.cnil.fr/en/> accessed 18 January 2024.

privacy design strategies, patterns and PETS in its "Guide to Privacy by Design".[15] Along the same lines, the Norwegian Datatilsynet offers guidance on the measures that can be implemented at every stage of the software development lifecycle.[16] Many other NSAs provide comparable resources, an overview of which would drastically extend an already long piece.

Administrative decisions reflect the diversity of the measures NSAs can require controllers to implement, ranging from punctual adjustments to a complete revamp of their processing operations. While it would be fairly unrealistic to detail them all in this section, the column "Type(s) of measure(s)" in the sheet "Components of DPbD" provides plethora of concrete examples. That said, most measures tend to pursue comparable–if not identical–goals. If their scope and implementation vary, it is therefore possible to cluster most of them into general categories.

Decisions pointing out a lack of, or an insufficient, risk assessment process represent the largest category. In case IN 20-7-4, for instance, the DPC noted that, by making child users' contact information publicly available upon switching to an Instagram business account, Facebook Ireland Limited–now Meta Platform Ireland Limited–had failed to "properly take into account the risks posed to the rights and freedoms of child users when implementing measures to ensure its compliance with the GDPR". The Polish UODO held a similar reasoning in DKN.5101.25.2020 when reprimanding a waste management company for failure to integrate the human factor, "which is one of the sources of risks", in its risk assessment process when printing a list containing the addresses of people in quarantine for a confirmed infection to COVID-19 (p. 11). It reached the same conclusion with regard to the Warsaw University of Life Sciences in ZSOŚS.421.25.2019 (p. 28).

Many decisions also criticise the lack of appropriate documentation. In 138/2022, the APD required a private individual operating cameras partially pointed toward their neighbours to maintain a register of imaging activities as "a basis to comply with the accountability obligation provided for in Articles 5(2) and 24(1) GDPR" (para 46). When assessing twelve personal data breaches imputed to Meta Platform Ireland in IN 18-11-5, the DPC considered that documents in the form of internal "Wiki" available on the company's intranet were not, "in and of themselves", appropriate to demonstrate compliance with its security and accountability obligations under the GDPR if these are limited to "high level overview" of the measures at stake (para 91). The same goes for any other type of document that merely describes a compliance or security programme, if it is not paired with concrete evidence as to how the actual risk assessment process has been performed (paras 93-94, 104-108). The Commissioner took a similar position in IN 19-7-2, where it considered that the Irish Credit Bureau had failed to demonstrate compliance with the Regulation by not maintaining a record of the code changes implemented over time, together with the results of the mandatory testing and evaluation carried out before their implementation (paras 7.4-7.5).

The absence of internal policies or procedures governing the collection and use of personal data also frequently appears among the grievances directed at controllers. In decision NAIH/2019/51/11, the NAIH fined an employer for not having adopted internal rules on the archiving of former employees' email accounts, leading to the backup and retention of a professional mailbox that also contained private emails. These rules, underlined the NAIH, should at least cover (i) whether professional e-mail accounts can be used for private purposes, (ii) what part of the mailbox will be backed up in the event of an employee leaving the company, as well as for how long its content will be retained by the former employer, and (iii) whether and how employees can review the sorting and backup process. The Hungarian authority issued comparable findings in NAIH/2019/769. The Norwegian Datatilsynet, for its part, progressively fleshed out a solid jurisprudence on credit assessment procedures. In decision 21/02293-10, it argued that these should describe when and how credit information can be obtained and how access is to be provided (point 4.4,

15 Agencia Española de Protección de Datos, 'A Guide to Privacy by Design' 1 <https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf> accessed 19 January 2024. See also the controls designed to address the risk inherent to the processing of personal data listed in Agencia Española de Protección de Datos, 'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales' Section VIII <https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf> accessed 19 January 2024.

16 Datatilsynet, 'Software Development with Data Protection by Design and by Default' <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/> accessed 19 January 2024; See, more specifically, the section on "Design" and the suggested "checklist for content in the design activity".

p. 4). Such a procedure should also clarify the exact circumstances under which a credit check can be carried out and who is responsible for that assessment (point 5.2, p. 5). Finally, it should guarantee that the correct customer is credit-checked by verifying their address before proceeding with the actual credit check (point 6.3, d), p. 9 and point 6.4, p. 12).[17]

Several decisions also insist on the importance of technical and organisational access control measures. In decision 9790365, the Garante fined the Azienda sanitaria universitaria Friuli Centrale for failing to restrict access to patients' data to the personnel actually in charge of their treatment, instead using a single authorisation profile shared by all its employees (p. 10). In decision 9685994, it also fined Deliveroo Italy for having configured its order, communication and payment management systems in such a way as to allow operators to "switch through simple functions from one system to another" and access all the data related to all riders regardless of the order (p. 14). Besides, the design of the order management system allowed Italian operators to consult the data of riders active in other countries, while foreign operators also had access to the data of Italian riders (p. 15). In decision 20/01813-4, the Norwegian Datatilsynet fined St. Olavs Hospital for failing to log the activities performed on specific files. This, it stated, made it impossible "to confirm or verify whether staff had access" to the documents at stake, and "to detect future unauthorised access that could compromise the personal data of the patients" (p. 10). It held a similar reasoning in 20/01879-7.

Encryption, either in transit or at rest, is also a measure frequently imposed by NSAs to guarantee an appropriate level of security. In decision 127/2022, the APD fined a medical laboratory for failure to use HTTPS on its website, despite being used by doctors to retrieve the results of their patients' medical analyses.[18] This, concluded the Belgian authority, paved the way for "man-in-the-middle attacks" since mere HTTP does not allow for the authentication of the website through a server-side digital certificate (paras 20-33). It also underlined the importance of setting up a robust two-factor authentication system alongside a secure communication protocol (para 34). In its Manx Care decision, the Isle of Man Information Commissioner regretted the lack of encryption solution for emails or attachments sent internally within a health institution, "including to any gov.im email address" (para 17 of the penalty notice). Along the same lines and in decision DKN.5131.22.2021, the Polish UODO fined the President of the Zgierz District Court for the loss, by a probation officer under its supervision, of an unencrypted memory stick leading to a breach of sensitive data affecting 400 individuals (pp. 12-13).

Regular testing and evaluation are also critical in ensuring the sustainability and efficiency of the measures implemented pursuant to Articles 24(1) and 25(1) GDPR. The Finnish Tietosuojavaltuutetun toimisto stressed that point in case 6097/161/21 by sanctioning Otavamedia–a major actor in the Finnish media landscape–for not having ensured, through regular testing, the proper functioning of the main communication channel used by data subjects to exercise their rights. In this case, a change of email service provider interrupted the routing of emails to the customer service contact system, resulting in data protection queries and requests not being forwarded for seven months. Against that background, the Finnish authority highlighted the importance of adopting a test plan and creating test cases before and after switching to a new service provider (pp. 5, 7, 29-33). In case DKN.5130.2215.2020, the Polish UODO sanctioned a processor for failure to test, during the development phase, the security functions of a new database designed to speed up the retrieval of documents by the controller, the wrong configuration of which led to a data breach affecting 120,428 data subjects.

Lastly, many decisions outline the importance of training and awareness raising activities. In its Decision of 31 May 2022 issued in the context of the loss of a diploma by a school during its relocation, the Croation Agencija za zaštitu osobnih podataka ("AZOP") insisted on the need to "continuously educate the persons involved in the processing of personal data, primarily in terms of their obligations to safely manage these documents in such a way that any possibility of loss or disappearance is minimised" (p. 4). In the same vein, ΑΠΟΦΑΣΗ 50/2021 was the opportunity for the Greek Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα

17 A similar reasoning can be found in decisions 20/02066, 21/02504-7, 20/04401-11, 20/02375-9, 20/02172-4, 20/01896-3, and 20/02225-6. The Personvernnemnda, responsible for handling appeals lodged against decisions from the Datatilsynet, confirmed these conclusions in PVN-2022-03.

18 The Garante emphasised, on multiple occasions, the importance of using the HTTPS protocol over the older, unencrypted HTTP alternative. See 9790365, 9698724, 9685922 and 9591223.

("HDPA") to underline the role of support groups and training sessions in assisting teachers with the identity verification process used to limit third party access to digital classes amidst the COVID-19 pandemic. The authority also noted the importance of providing evidence that information and awareness-raising actions have been systematically implemented (para 18). In Hora Credit IFN, the Romanian Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal ("ANSPDCP") also emphasised the importance of "training the persons processing personal data under the authority of the controller", arguing that this would have contributed to preventing the sending of credit-related documents to the wrong email address (p. 1).

2.1.2 Appropriate measures

Controllers must also ensure that these measures are "appropriate". In the words of the EDPB, that they are "suited to achieve the intended purpose", and "implement the data protection principles effectively". The requirement of appropriateness is therefore "closely related" to that of effectiveness.[19] The Board insisted on that point in its Binding Decision 2/2023, in which it expressed serious doubts as to the appropriateness of the *ex-ante* and *ex-post* age verification processes implemented by TikTok to bar access to the platform to children under 13 years of age (paras 243-245). More specifically, noted the Garante in its relevant and reasoned objections on the draft decision, the age gating system based on self-declaration "could be easily dodged", which the Board regarded as a relevant factor when assessing its effectiveness (para 227). Since these properties must be assessed against the purposes pursued by the measure, it is therefore necessary to, first, assess the risks posed by the processing at stake by considering the elements detailed in Section 3 and, second, determine the objectives to be achieved when mitigating these risks. Controllers then enjoy a wide margin of manoeuvre when it comes to the actual measures to be implemented pursuant to Articles 24(1) and 25(1), as long as these ensure the "effective protection of personal data throughout the Union".[20]

In decision DI-2019-3840, the Swedish Datainspektionen concluded that Sahlgrenska University Hospital had failed to precisely delineate who needed access to what data in which context, and to take into account the specific circumstances related to the patients, such as the existence of protected personal data, public figures or otherwise particularly vulnerable persons. Short of such analysis, the hospital was not in a position to design an access control system able to achieve the objective outlined above, as the permissions granted to the personnel were way too broad (pp. 19-25). In decisions 4356/532/19, 8211/161/19 and 834/532/18, the Finnish authority noted that, indeed, data protection by design "does not require the adoption of any specific measures, but rather that the measures and safeguards chosen must be appropriate to the implementation of the data protection principles in the specific processing operation in question" (pp. 11, 11 and 10, respectively). The counterpart, of course, is the obligation to ensure that these countermeasures remain "appropriate" despite changes in the scope or context of the processing. As a relative concept, it requires controllers to scale or adapt these measures should the level of risks increase or decrease over time.[21] If identifying and mitigating the risks to data subject's fundamental rights and freedoms is an intrinsically dynamic and contextual exercise, so is the implementation of "appropriate" measures, which "is at the heart of the concept of data protection by design".[22]

19 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 8.

20 Recital 11 GDPR. The CJEU has used the notion of "effective protection" on multiple occasions, notably when arguing in favour of the broad interpretation of the concept of "controller". See *Fashion ID GmbH & co.KG v Verbraucherzentrale NRW eV*, Case C-40/17 [2019] electronic Reports of Cases (ECLI:EU:C:2019:629) para 66; *Tietosuojavaltuutettu*, Case C-25/17 [2018] electronic Reports of Cases (ECLI:EU:C:2018:551) para 66; *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 28; *Google Spain v Agencia Española de Protección de Datos (AEPD)*, Case C-131/12 [2014] electronic Reports of Cases (ECLI:EU:C:2014:317) para 34.

21 The EDPS already pointed out the importance of "scalability" at the earliest stage of the reform process. See European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Data Reform Package' para 174 <https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 20 January 2024.

22 See, on that point, European Data Protection Board, 'Guidelines 4/2019' (n 12) para 13.

2.1.3 Obligation of result or of means?

The GDPR does not specify whether data protection by design must be regarded as an obligation of "result" or of "means". This, however, significantly impacts the burden of proof and the margin of appreciation that controllers enjoy when substantiating that obligation. In the event of an obligation of result, controllers would be bound to achieve the objective set out in Article and 25(1), namely to implement appropriate measures to ensure compliance with the provisions contained in the Regulation. Non-compliance would therefore be assumed from the mere failure to achieve that goal, with no possibility for controllers to reverse that presumption besides force majeure. In the event of an obligation of means, however, controllers would only be required to do their best to comply. That is, to make the same reasonable efforts as another controller would under similar circumstances. Compared to an obligation of result, establishing non-compliance with an obligation of means would then require demonstrating that the controller was not diligent enough in its attempt to act upon its obligations.

Lina Jasmontaite and her co-authors have interpreted the "effectiveness" requirement as an indication of an obligation of result, arguing that controllers are free to implement the measures of their choosing "provided that they actually achieve [the result of data protection by design]".[23] That interpretation, I argue, follows from a restrictive conception of "appropriateness" and does not stand up to closer scrutiny. Determining whether a measure is "appropriate" indeed requires to consider a series of factors, including the nature of the processing and the state of the art, to assess whether the controller has acted diligently to mitigate the risks posed by the processing. Quite logically then, determining whether controllers have actually *achieved* the objective pursued by Article 25(1) calls for a similar analysis. If the principle of accountability has shifted the initial burden of proof on to the controller, it remains up to data subjects or supervisory authorities to deconstruct that position later on, and demonstrate that the controller *has not* acted diligently in this particular case. Which means, in turn, that so was its obligation pursuant to Article 25(1). Considering data protection by design as an obligation of result therefore disregards the dynamic nature of the assessment that must precede any claim as to the (in)appropriateness of a specific measure.

The CJEU recently embraced that exact reasoning in Case C-340/21, in which it clarified that "the appropriateness of such measures must be assessed in a concrete manner, by assessing whether those measures were implemented by that controller taking into account the various criteria referred to in [Articles 24 and 32 GDPR] and the data protection needs specifically inherent to processing concerned and the risks arising from the latter". As such, held the Court, these provisions "cannot be understood as meaning that unauthorised disclosure of personal data or unauthorised access to such data by a third party are sufficient to conclude that the measures adopted by the controller concerned were not appropriate, within the meaning of those provisions, without even allowing that controller to adduce evidence to the contrary". Should data protection by design be considered as an obligation of result, and an irrefutable presumption be accepted, controllers would simply be deprived of that possibility.[24]

The WP29 had also positioned itself in favour of that approach, stating that "rather than being an obligation of goal, these provisions [i.e., Articles 25 and 32 GDPR] introduce obligations of means, that is, the controller must make the necessary assessments and reach the appropriate conclusions". "The question that the supervisory authority must answer", it argued, is therefore "to what extent the controller 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation".[25] Back in 2014, the CNIL defended a similar position when comparing the obligation to notify a data breach to the obligation of security, and stated that the

23 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, 174 <https://edpl.lexxion.eu/article/EDPL/2018/2/7> accessed 19 January 2024. They also note that "in terms of enforcement, the requirement that the DPbD [...] measures be *effective* will be the one that allows supervisory authorities to measure compliance with DPbD obligations". This, they argue, "is also the legal requirement that indicates th[at] DPbD obligation is one 'of result' and not one of 'best efforts'".

24 *VB v Natsionalna agentsia za prihodite* (n 7), respectively paras 30, 31 and 32.

25 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> accessed 20 January 2024.

former was an obligation of result distinct from the latter, itself an obligation of means.[26] More recently– but not referring so clearly to an "obligation of means"–, the DPC highlighted in decision IN 21-4-2 that "Article 25(1) GDPR does not impose a *strict liability* standard" (emphasis added). As a result, it added, "the requirement to implement the principles in an effective manner does not mean that any undesired outcome in respect of the data protection principles will necessarily be indicative of an underlying infringement of Article 25(1) GDPR" (para 153). If the notion of strict liability relates to the specificities of the tort law regime rather than to the burden of proof, the thrust is nonetheless similar in that it calls, *a contrario*, for a risk-based approach. Looking at French legal literature, Céline Castets-Renard also builds on the assessment criteria inherent to Article 25(1) to plead in favour of its qualification as an obligation of means.[27]

2.2 Of technical and organisational nature

These appropriate measures, clarify Articles 24(1) and 25(1) GDPR should be "technical" and "organisational" in nature. While, there again, the Regulation does not provide any definition of these qualifiers, Dag Wiese Schartum rightfully observes that the consistent use of that vernacular throughout the text suggests that it should be read and understood as a homogeneous concept.[28]

2.2.1 Technical measures

As pointed out in literature, "technical" should not be confused with "technological", as the former is broader than the latter.[29] Indeed, technology must not always be part of the measure, even though contrasting "technical" with "organisational" within the same sentence seems to suggest the existence of two mutually exclusive and collectively exhaustive groups. Unfortunately, some NSAs seem to endorse that binary interpretation in their case law by qualifying as "technical" some measures that integrate a "technological" component. This is the case, for instance, for encryption in decisions 9808698, 9806053 and 9782890 from the Garante (pp. 9, 9 and 8, respectively), for the purchase of a high-end edge device and a set of licences extending the device's security capabilities in decision DKN.5130.2559.2020 from the UODO (p. 8), and for the testing and patching of software vulnerabilities in decision 20/02376-5 from the Datatilsynet (p. 8). Sticking to such a narrow interpretation would, as detailed below, pave the way for controllers to escape their responsibilities by arguing that a given measure does not fall within either one of these categories. In the context of data protection by design, the notion of "technical", I argue, should rather be understood as "relating to the knowledge and methods of a particular subject",[30] or "marked by or characteristic of specialization".[31] A "technical measure" would therefore encompass any solution, involving technology or not, that draws from a specific field of expertise to overcome, in this case, a data protection challenge.[32]

26 *Délibération de la formation restreinte n° 2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société x.*, mentioned by Randy Yaloz, 'Conformité au RGPD : obligation de moyen ou de résultat' (*ELC Paris*, 15 September 2019) <https://elc-paris.com/conformite-au-rgpd-obligation-de-moyen-ou-de-resultat/> accessed 20 January 2024.

27 Céline Castets-Renard, 'La protection des données personnelles dans les relations internes à l'Union européenne', *Répertoire de droit européen* (Dalloz 2018) para 181 <https://www-dalloz-fr/documentation/Document?id=ENCY/EUR/RUB000406> accessed 21 January 2024.

28 Schartum (n 11) 291. He also notes that, in total, fourteen provisions refer, word for word, to the notion of "technical and organisational measures", namely Articles 4(5), 5(1)e, 14(5)b, 22(3), 22(4), 24(1), 24(1), 25(1), 28(1), 28(3)e, 28(4), 32(1), 32(1)d and 36(3)c. See Schartum (n 11) 294.

29 Mentioned by Lee A Bygrave, 'Data Protection by Design and by Default' in Sacha Garben and Laurence Gormley (eds), *Oxford Encyclopedia of European Union Law* (2023) para 16 <https://opil.ouplaw.com/display/10.1093/law-oeeul/law-oeeul-e138> accessed 20 January 2024.

30 *Cambridge Dictionary*, 'Technical' (Cambridge University Press, 2024) <https://dictionary.cambridge.org/dictionary/english/technical> accessed 15 February 2024.

31 *Merriam-Webster Dictionary*, 'Technical' (Merriam-Webster, 2024) <https://www.merriam-webster.com/dictionary/technical> accessed 15 February 2024.

32 One could argue that the role of "technical" as the main qualifier for those "measures" is also reflected in the title of the German version of Article 25 GDPR, which reads "Datenschutz durch *Technik*gestaltung und durch datenschutzfreundliche Voreinstellungen" (emphasis added). Although, as noted by Marit Hansen, this could merely be attributed to the importance of "Datenschutz durch Technik", a concept "introduced in the mid-1990ies to denote the work on Privacy Enhancing Technologies". See: Marit Hansen, 'Data Protection by Design and by Default à La European General Data Protection Regulation' in Anja Lehmann and others (eds), *Privacy and Identity Management. Facing up to Next Steps* (Springer International Publishing 2016) 31 <https://link.springer.com/chapter/10.1007/978-3-319-55783-0_3> accessed 15 February 2024.

2.2.2 Organisational measures

Often overlooked in favour of the "technical" aspect,[33] organisational measures also play a critical role in ensuring compliance with the provisions stemming from the Regulation. While the former tend to focus, as criticised above, on the *technological* dimension, the latter refer to everything that "is related to the planning of an activity or an event".[34] "Assigning tasks, functions [and] responsibilities to someone or a department", notes Dag Wiese Schartum, "are central examples of 'organisational' [measures]". These measures therefore "embrace more than the design and operation of software or hardware", and also "encompass business strategies and other organisational-managerial practices".[35] These would typically cover the allocation of responsibilities for the performance of a DPIA and for the management of data subject's rights.

Many other examples can be found in administrative case law. In decision IN 21-4-2 issued against Meta, the DPC noted that setting up a team dedicated to the identification and mitigation of the reidentification risks arising from the scraping of publicly available information "would have been a relevant organisational measure" (para 144). In the context of controller-processor relationships, the Polish UODO also emphasised that "the oversight and monitoring of outsourced systems is *one of the primary organisational measures* that the controller should effectively implement to ensure the security of personal data in accordance with the requirements under Regulation 2016/679" (p. 20, emphasis added). And so are the training and education of the staff whose functions regularly involve the processing of personal data, as underlined in decisions DKN.5131.22.2021 (p. 11) and DI-2019-3840 (p. 26).

2.2.3 Too limiting really?

Schartum builds on public governance literature to suggest three additional types of measures that controllers could implement as part of their obligations under Articles 24(1) and 25(1), namely (i) legal, (ii) economic and (iii) educational measures. However, supplementing the original wording of Articles 24(1), 25(1) and 32(1) GDPR with additional categories amounts to acknowledging the limited scope of the notions of "technical" and "organisational", which, I argue, risks watering down the level of protection afforded to data subjects by putting too much emphasis on the nature of the measures rather than on their objective. The latter should be the decisive criterion in light of assessing the relevance and appropriateness of a given measure. A restrictive interpretation of these qualifiers would allow controllers to rely on a semantic argument to limit their responsibilities to *only* the implementation of measures that fall within the remit of what is commonly understood as "technical" or "organisational". This would run contrary to the objective of the Regulation, which is to "protect [the] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (Article 1(1) GDPR).

Wrapping up, there are essentially two ways to understand the terms "technical" and "organisational" without lowering the standard of protection set by the Regulation, both leading to the same consequences for controllers: either by focusing on "technical" as the overarching qualifier and interpreting it in a broad manner, as suggested above; or, if reading "technical" as "technological"–*quod non*–, by considering both qualifiers as non-exhaustive examples of the type of measures that controllers can implement under Articles 24(1) and 25(1) GDPR. In any case, the nature of the measures should not be a ground for controllers to limit the extent of their obligations pursuant to data protection by design. Schartum already leaned toward a similar interpretation when he noted that "interpreting 'technical and organisational measures' in line with common parlance cannot be seen as an exhaustive indication of which measures may be legally required on the basis of the GDPR".[36] While he also wondered whether "a legal obligation exists to consider measures that are clearly not in harmony with common understanding of 'technical' and 'organisational'", I would argue that such an obligation *does* exist, as concluding otherwise would significantly weaken the impact of Articles 24(1) and 25(1) GDPR.

33 Sophie Stalla-Bourdillon and others, 'Data Protection by Design: Building the Foundations of Trustworthy Data Sharing' (2020) 2 Data & Policy 1, 4 <http://www.cambridge.org/core/journals/data-and-policy/article/data-protection-by-design-building-the-foundations-of-trustworthy-data-sharing/4A4579B8FD774F7CDF8A1867A839B5FB> accessed 22 February 2024.

34 *Cambridge Dictionary*, 'Organizational' (Cambridge University Press, 2024) <https://dictionary.cambridge.org/dictionary/english/organizational> accessed 22 February 2024.

35 Bygrave (n 9) 115.

36 Schartum (n 11) 295.

2.3 To ensure and demonstrate compliance with the GDPR

The goal that these "appropriate measures" must pursue slightly differ depending on the provision at stake. While Article 24(1) obliges controllers to "ensure and be able to demonstrate that [the] processing is performed in accordance with this Regulation", Article 25(1) uses a more convoluted wording and requires the said measures 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". This ties back to the delicate issue of the *material scope* of data protection by design, i.e., the *actual* principles and rules that the measures implemented pursuant to Articles 24(1) and 25(1) should give effect to. That ambivalence ranks relatively high in the list of criticisms formulated against the EU conception of data protection by design.[37]

This raises two questions. First, whether the measure referred to in Articles 24(1) and 25(1) should *only* substantiate the general principles listed in Article 5, or rather strive to ensure and demonstrate compliance with *all* the obligations contained in the Regulation (Section 2.3.1). Second, and assuming that the answer to the above question leans towards a broad interpretation, whether these measures should go beyond what is *explicitly* required by the Regulation to also mitigate all the risks posed by the processing *for data subject's fundamental rights and freedoms* (Section 2.3.2).

2.3.1 Only the principles, or the entire Regulation?

Answering the first question is rather straightforward. First thing first, the use of "such as" in Article 25(1) suggests that "data minimisation" is only one example of the principles that the measures must substantiate. In that sense, there is absolutely no doubt that data protection by design covers *at least* all the general principles listed in Article 5.[38] Whether Articles 24(1) and 25(1) also extend to the other provisions contained in the Regulation is, as noted in legal literature,[39] equally trivial. Both provisions indeed *explicitly* refer to that broader objective; Article 24(1), by specifying the obligation to ensure that the processing is performed "in accordance *with this Regulation*", and Article 25(1), by broadening its objective to also encompass measures designed to "integrate the necessary safeguards into the processing *in order to meet the requirements of this Regulation*" (emphasis added).

If Articles 24(1) and 25(1) indeed require controllers to implement *all* the provisions of the Regulation *by design*, one must acknowledge that their positioning within the text is confusing. Indeed, responsibility and data protection by design are but two of the eight obligations listed under Chapter IV, Section I entitled "General obligations". This is at odds with their role as transversal requirements, which a dedicated Section within the Regulation would have better reflected. That unfortunate positioning has led many scholars to question their added value. Ari Waldman, for instance, notes that "Article 25 is repetitive of other sections of the GDPR and has no identity of its own".[40] In that, he is joined by Rubinstein and Good, who wonder–if in a less conclusive way–about "the specific contribution of Article 25 to these existing obligations".[41]

It is true that Articles 24(1) and 25(1) repeat provisions contained elsewhere in the Regulation. Yet, discarding their added value based on such overlaps would disregard what these provisions bring to the table *besides* these repetitions. Indeed, data protection by design is not *only* about the implementation of measures to ensure compliance with the Regulation, but adds two crucial components. First, the risk-based approach that requires controllers to tailor the extent of their compliance exercise based on a series of variables, as discussed extensively in Section 3. And, second, the timing aspect that calls for the integration of these considerations as early as possible in the development process, as detailed in Section 4.

37 See, on that point, the second of the five weaknesses pointed out by 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, 41 <http://academic.oup.com/idpl/article/10/1/37/5607285> accessed 22 February 2024.

38 Bygrave (n 8) 115, goes as far as considering such a controversy a "moot point and arguably of academic interest only, as the pith of such principles is adequately covered by Article 5, at least at an operational level".

39 See, for instance, Jasmontaite and others (n 23) 175, who notes that Article 25(1) is essentially "a longer, complicated way to convey a message than saying that *the appropriate measures must be designed to ensure compliance with the GDPR*" (emphasis in original).

40 Waldman (n 10) 157.

41 Rubinstein and Good (n 37) 40.

While the existence of repetitions is beyond contest, these, I argue, are purely illustrative and give more meat to an obligation that goes far beyond "parroting" the remainder of the Regulation. In his analysis, Waldman seems to focus on the similarities between Article 25(1) and the other obligations stemming from the GDPR, rather than on what makes it a standalone provision. That he reaches such a conclusion is therefore not surprising. What is, though, is that his reference to the "effet utile" as a method of interpretation of EU Law did not lead him to consider these additions. As he correctly points out,[42] one of the implications of that principle is that the EU legislator must avoid duplications, so that no provision of EU law is redundant or bears the exact same meaning as another provision that belongs to the same normative text.[43] Interpreting Article 25(1) in light of the "effet utile" doctrine should therefore have resulted in extracting its intrinsic added value when compared to the other provisions of the Regulation. Contrary to what many scholars have argued during and after the adoption of the GDPR,[44] I believe that the *material scope* of Article 25(1), when read in combination with the other pieces of the data protection by design puzzle, is sufficiently clear.

Even if these overlaps would undermine the clarity of Article 25(1)–*quod non*–, a teleological reading of that provision through the lens of the preparatory works – an option also suggested by Waldman –[45] should point to the same conclusion. As detailed in the first paper, the EU legislator has always ambitioned the adoption of a flexible regulatory framework shifting the burden of ensuring and demonstrating compliance on to controllers, while anchoring data protection considerations as early as possible in the development life-cycle. These objectives perfectly coincide with the two additional dimensions brought forward by Articles 24(1) and 25(1). In his piece, Waldman criticises Article 25(1) GDPR for not being "a faithful reflection of privacy by design literature".[46] While I agree with that observation, I do not consider that as an issue. Instead of transposing a pre-established conception of "privacy by design" that would have inherited years of conceptual controversies, the EU legislator took inspiration from that rich background but came up with its own "codification" in the form of "data protection by design": a *sui generis* concept that bears a specific meaning within the context of the Regulation.

2.3.2 Only the Regulation, or...

Now that the above paragraphs have clarified that the measures to be implemented are not limited to the general principles listed in Article 5 GDPR, but must give effect to *all* the rules stemming from the Regulation, comes the second part of the reasoning. That is, whether these measures should only substantiate what is *explicitly* contained in the Regulation, or also serve a broader purpose. Answering that question calls for a two-step reasoning.

First, it requires dissecting the very objective that these "appropriate technical and organisational measures" must pursue. As noted earlier, Article 24(1) requires them "to ensure and to be able to demonstrate that processing is performed in accordance with *this Regulation*", while Article 25(1) states that they shall "integrate the necessary safeguards into the processing in order to meet the requirements of *this Regulation* and protect the rights of data subjects".

42 Waldman (n 10) 161.

43 Koen Lenaerts and Jose A Gutierrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 Columbia Journal of European Law 3, 17 <https://heinonline.org/HOL/P?h=hein.journals/coljeul20&i=183> accessed 24 February 2024.

44 Rubinstein and Good (n 37) 41; Waldman (n 10) 148, 149, 153, 159; Bincoletto (n 8) 168; Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 13 <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipy002/4960902> accessed 22 February 2024; Bygrave (n 9) 117; Koops and Leenes (n 8) 161; Ira S Rubinstein and Nathaniel Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 Berkeley Technology Law Journal 1333, 1334 <https://heinonline.org/HOL/P?h=hein.journals/berktech28&i=1367> accessed 22 February 2024; Hornung (n 8) 75.

45 Waldman (n 10) 165. The Professor indeed notes that "[o]nly a teleological interpretation, which is difficult to predict, can empower Article 25(1) to require real, meaningful, technological, and structural changes inside companies that create and leverage data collection tools".

46 Waldman (n 10) 158.

At first sight, the reference to the requirements of "this Regulation" in both provisions seems to favour a restrictive reading of their material scope of application. Yet, that conclusion only holds true if what the GDPR "requires" is, in fact, limited to complying with the finite set of principles and rules it contains. Article 1(2) recalls that the GDPR aims to "protect [the] fundamental rights and freedoms of natural persons and *in particular* their right to the protection of personal data". Recital 4 adds that the Regulation "observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, *in particular* the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity". What the GDPR "requires", then, is that controllers mitigate all the risks to the data subject's fundamental rights *arising from* the processing of the latter's personal data. The same goes, arguably, for the said measures.

This ties back to the very nature of the GDPR as a legislative instrument, i.e., a piece of secondary EU law that operationalises that overarching goal by laying down rules to protect *all* natural persons' fundamental rights, *including but not limited to privacy and data protection*, in the context of *the processing of their personal data*. This suggests that "data protection" can either refer to the set of implementing rules contained in Directives and Regulations, or to its fundamental right component. While the recognition of data protection as an independent fundamental right in Article 8 CFREU has led some authors to question its exact added value,[47] the EU legislator considered it sufficiently important to warrant a dedicated mention in Article 16 the Treaty on the Functioning of the European Union. Bottom line being, the GDPR, and therefore the "appropriate technical and organisational measures" that controllers must implement pursuant to Articles 24(1) and 25(1), should not only strive to protect data subject's fundamental right to data protection–whatever it adds to the EU fundamental right ecosystem–but, more importantly, also guarantee the respect for other fundamental rights such as privacy, freedom of thought, freedom of expression, freedom to choose an occupation, non-discrimination or cultural, religious and linguistic diversity.

Several hints scattered across the Regulation support such a broad interpretation of the material scope of data protection by design. As noted above, Article 25(1) requires the said measures to allow controllers to both "meet the requirements of this Regulation *and* protect the rights of the data subjects". Interpreting "the rights of the data subjects" as a reference to data subject's rights within the meaning of Articles 15 to 22 would lead to a strange conceptual overlap since "the requirements of this Regulation" already cover compliance with these provisions. Such a reading also transpires from Recital 78, which justifies the need for "appropriate technical and organisational measures" by referring to "the protection of the rights *and freedoms* of natural persons". The use of the term "freedoms" in the Recital that directly complements Article 25(1) lifts any remaining doubt as to the interpretation to be given to the notion of "rights of the data subjects". This vernacular directly builds on the wording of Article 8(2) ECHR, and is abundantly used throughout the Regulation itself to refer to *fundamental* rights and freedoms.[48] The "rights of the data subjects" should therefore be understood as referring to all their *fundamental rights*, that controllers should guarantee through "appropriate measures" when processing their personal data. The EDPB has positioned itself in favour of that broad interpretation when it stated that "the data protection principles are in Article 5 [and] the data subjects' rights and freedoms are the fundamental rights and freedoms of natural persons

47 Among the many authors that have contributed to that debate, I would more specifically point to Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes and others (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures*, vol 36 (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-50796-5_1> accessed 25 February 2024; Orla Lynskey, 'Deconstructing Data Protection: The "added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International & Comparative Law Quarterly 569 <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/deconstructing-data-protection-the-addedvalue-of-a-right-to-data-protection-in-the-eu-legal-order/95BD4CCF4670466FD4F6EBAD7DDB4E76> accessed 25 February 2024; Gloria González Fuster, 'EU Fundamental Rights and Personal Data Protection', *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, Cham 2014) <https://link.springer.com/chapter/10.1007/978-3-319-05023-2_6> accessed 25 February 2024; Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 Computer Law & Security Review 522 <https://linkinghub.elsevier.com/retrieve/pii/S0267364913001325> accessed 25 February 2024.

48 The wording "fundamental rights and freedoms" can be found in Recitals 2, 3, 4, 10, 16, 47, 51, 69, 102, 109, 113, 166, 173 and Articles 1(2), 4(24), 6(1)f, 23(1), 45(2)a, 50(b), and 51(1).

whose protection is named in Article 1(2) as the objective of the GDPR".[49] And so has the EDPS, when it underlined that "the assets to protect are the individuals whose data are processed and in particular their fundamental rights and freedoms".[50]

Second, it requires to assess whether the rules contained in the Regulation are exhaustive. Now that the above paragraphs have clarified that the measures to be implemented pursuant to Articles 24(1) and 25(1) should protect all data subject's fundamental rights with regard to the processing of their personal data, there are indeed two ways to reason about the *corpus* of rules contained in the Regulation.

Either we trust that the EU legislator has identified *all* the risks raised by the processing of personal data for data subject's fundamental rights, and elicited rules to overcome *each of them*. Under that interpretation, the provisions of the GDPR would constitute the product of a first risk management exercise performed by the legislator itself, which streamlines the one to be conducted by controllers (see layer 1 in Figure 1). In that case, implementing appropriate technical and organisational measures to comply with the provisions of the Regulation would, in theory, be sufficient to protect these rights. The risks controllers must mitigate thus strictly become the risks of *non-compliance* with the GDPR. Such is the position defended by Raphaël Gellert in his doctoral thesis,[51] and in a paper summarising his thoughts.[52] This is not to say that controllers are exempted from conducting their *own* risk management process, as the GDPR does not always prescribe how to operationalise its requirements. They must therefore still consider the broader risks to the data subject's fundamental rights when selecting the appropriate countermeasures, but can limit their exercise to substantiating the rules and principles listed the Regulation (see layer 2 in Figure 1). Building on the notion of "risk" as understood in ISO 31000:2018,[53] the processing of personal would be the "risk source",[54] non-compliance with the provisions of the GDPR the "event"[55], high risks for data subject's fundamental rights and freedoms the "consequence"[56], and actual compliance with the provisions of GDPR the "control".[57]

49 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 11.

50 European Data Protection Supervisor (n 1) para 28. Unfortunately, the accent is once again put on the general principles.

51 Raphaël Gellert, 'Understanding the Risk-Based Approach to Data Protection: An Analysis of the Links between Law, Regulation, and Risk' (Vrije Universiteit Brussel 2017) 201, Section 2.4.6.

52 Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 4 <https://www.sciencedirect.com/science/article/pii/S0267364917302698> accessed 25 February 2024. More specifically, he defends "a so-called 'compliance risk' at the heart of the GDPR, namely the chances that a given processing operation will not comply with the GDPR, as opposed to a notion of risk centred around the violation of the data subjects' rights and freedoms". "Thus", he posits at the beginning of his argumentation, "the lower the compliance or the higher the 'non-compliance event', the higher the (vernacular) risk (i.e., consequence or harm) to the data subjects' fundamental rights".

53 ISO 31000:2018 – Risk management – Guidelines (International Organization for Standardization 2018), available for purchase at <https://www.iso.org/standard/65694.html> accessed 10 March 2024. This standard replaces ISO 31000:2009. Clause 3.1 defines "risk" as the "effect of uncertainty on objectives" and notes that "An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats". It also states that a "risk is usually expressed in terms of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7)".

54 The "element which alone or in combination has the potential to give rise to risk" (Clause 3.4).

55 The "occurrence or change of a particular set of circumstances" (Clause 3.5). The ISO also notes that "An event can also be something that is expected which does not happen, or something that is not expected which does happen" and that "an event can be a risk source".

56 The "outcome of an event affecting objectives", noting that "a consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives" (Clause 3.6).

57 The "measure that maintains and/or modifies risk". The ISO also clarifies that "controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk" (Clause 3.8).

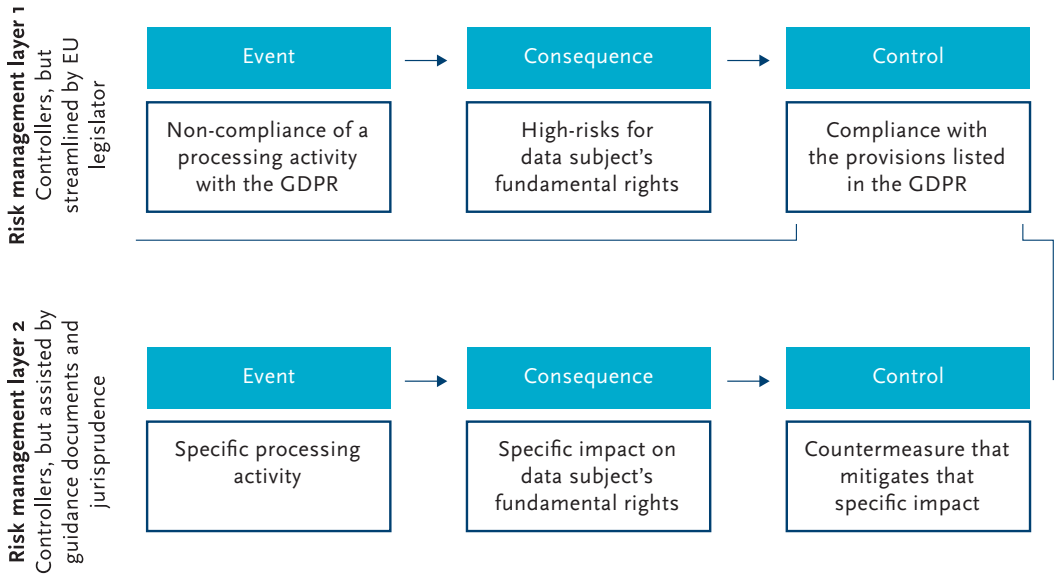

Figure 1. Scope of the risk management exercise if GDPR is exhaustive

Or we start from the postulate that the EU legislator has only identified *a subset* of the risks posed by the processing of personal data, and has only therefore come up with a *non-exhaustive* list of rules to protect data subject's fundamental rights. In that case, implementing appropriate technical and organisational measures to comply with the provisions contained in the Regulation would not be sufficient to protect all data subject's fundamental rights. The risks controllers must mitigate thus include, but also *exceed*, the risks of non-compliance with the Regulation. In that scenario, controllers are not only required to consider the risks for data subject's fundamental rights posed by their processing when substantiating the provisions contained in the GDPR (see layers 1 and 2 in Figure 1), but must *also* assess whether these risks warrant the implementation of countermeasures that are not explicitly mentioned in the text of the Regulation (see layer 3 in Figure 2). Reasoning so would broaden the scope of data protection by design, and therefore of controllers' risk management exercise. Referring, once again, to the terminology used in ISO 31000:2018, each processing would therefore constitute an "event", the impact it causes on a specific fundamental right the "consequence" and the countermeasure deployed to mitigate that impact the "control".

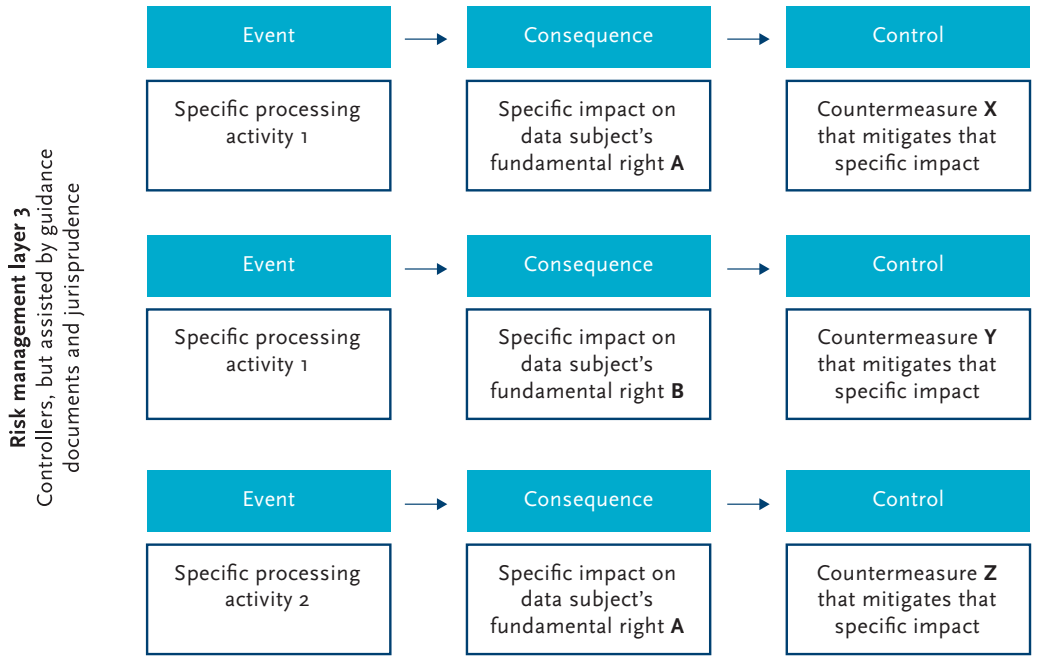

Figure 2. Scope of the risk management exercise if GDPR is not exhaustive

That second reading seems like the way to go, as many NSAs have already relied on the specific risks raised by certain processing operations to impose obligations that are not *explicitly* foreseen in the Regulation. In its decision PS/00120/2021, for instance, the AEPD prohibited Mercadona, a supermarket chain, from deploying a video surveillance system relying on facial recognition technology to identify and prevent individuals who have previously committed criminal acts such as theft from entering its physical shops. While the Spanish regulator abundantly documented the reasons why such a system could not be based on any of the lawful grounds listed in Article 6(1) nor any of the exceptions mentioned in Article 9(2) (pp. 66-81), and carefully detailed why it failed to meet the proportionality test (pp. 81-87), it justified its stance by referring to studies pointing toward the high error rate of facial recognition systems trained with limited and insufficiently diverse datasets. It considered such risk unacceptable since "inaccuracy is predictable from the very moment of the design of this type of information system" and "confusion with another person can lead to discrimination and social exclusion" (p. 95). This reads as a form of jurisprudential prohibition of facial recognition systems that are prone to statistical inaccuracies. In other words, a "rule" that, while not explicitly contained in the Regulation, is nonetheless necessary to guarantee data subjects' *fundamental right to non-discrimination* in the context of the processing of their personal data.

The countermeasure imposed on IAB Europe by the APD in Decision 21/2022 is another example of such a "para-GDPR" rule. Beside the breaches of principles and rules explicitly contained in the Regulation, the Belgian regulator also built on the security principle of Articles 5(1)f and 32 to oblige the company, as Managing Organisation and joint controller for the processing operations of the TC string, "to ensure that participants comply with the TCF Policies" (para 483). The APD supported its position by flagging that the so-called "TCF Vendor Compliance Programme" set up by IAB Europe was "permissive" rather than "dissuasive", as TCF participants could declare themselves in breach of the TCF Policies "up to three times without any form of sanction" (para 488). Again, this reads as an additional obligation for providers of technical frameworks designed to guarantee compliance with the GDPR to ensure, control and verify the proper implementation of their solutions by the implementing entities. This, argued the APD, is necessary to protect data subject's *fundamental rights to privacy and data protection*, "especially in view of the crucial role played by information and communication technologies in our society" (para 479).

The analysis of the notion of "risk" under the GDPR, read in light of these examples, suggests that the EU legislator did not, in fact, anticipate all the potential pairs of "events" and "consequences" and did not, as a result, come up with a definitive catalogue of measures to be implemented by controllers. Fortunately so, as this would have run contrary to its very purpose, i.e., providing a flexible and future-proof set of guarantees for data subjects' rights and freedoms. Putting the "risk" in "risk-based approach" will, in that sense, *always* require *a* form of risk management process. As such, data protection by design is also a Swiss knife for NSAs to gradually shape and orient what is expected from controllers in a wide range of scenarios.

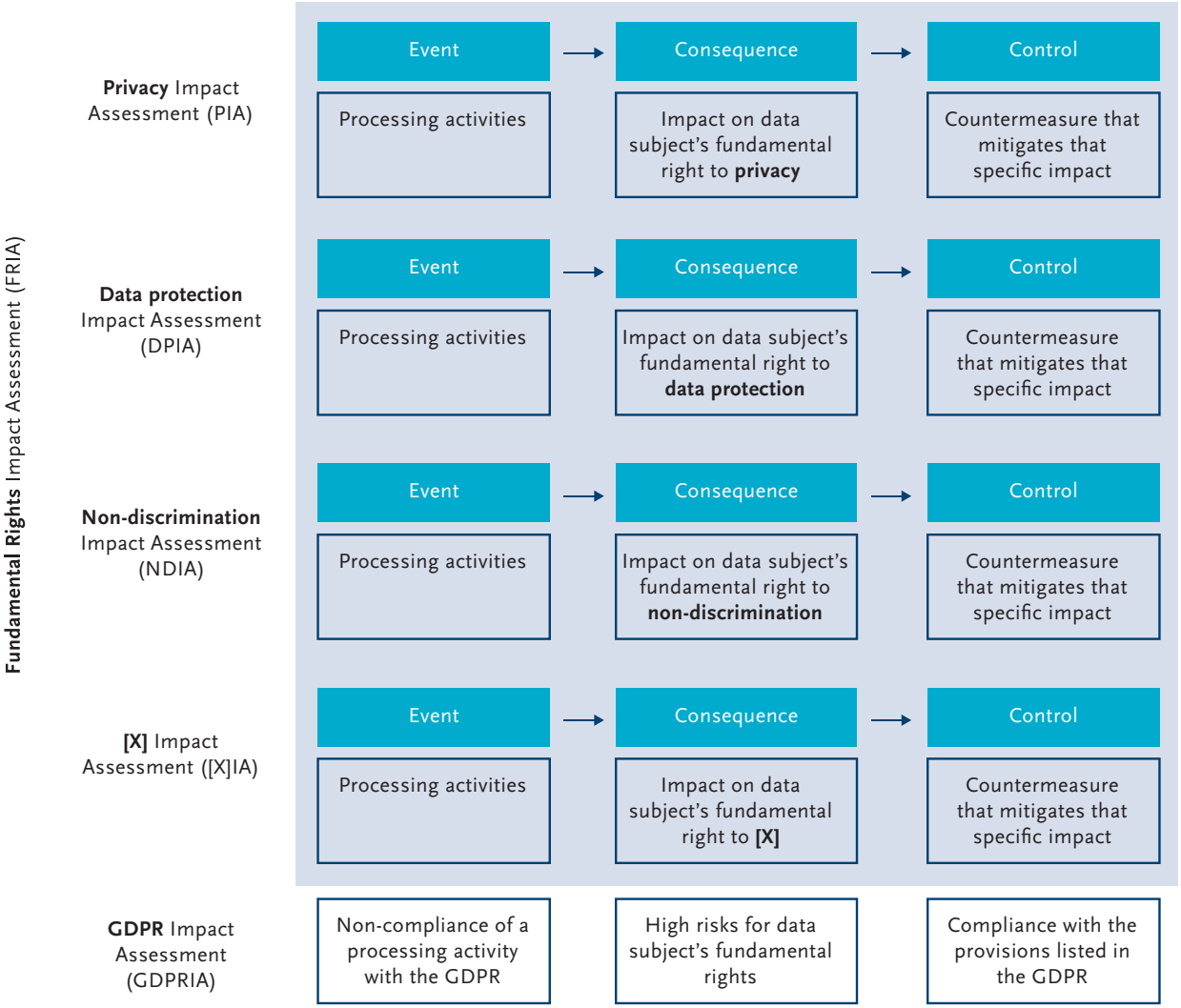

Figure 3. GDPRIA as a (partial) proxy to FRIA

2.3.3 The GDPR, a tinted window on the Charter

The discussion as to the material scope of data protection by design nicely sets the scene to transition to the distinction between the many forms of "by design" obligations and corresponding "impact assessments". If "privacy by design" and "data protection by design" have been used interchangeably before, and during the reform process,[58] the controversies outlined earlier in this paper have shed light on the importance to clarify the *object* of the assessment, i.e., what fundamental rights does the processing operations impact, and the *purpose* of the countermeasures to be implemented by controllers, i.e., how to appropriately mitigate that impact. Summarising all the above:

1. The goal of the Regulation is to protect all data subject's fundamental rights, including but not limited to privacy and data protection, in the context of the processing of their personal data (i.e., a *broad* interpretation of its objective).
2. Complying with the principles and rules it contains is a mandatory *starting point* (as illustrated in "Risk management layer 1" in Figure 1), but controllers must *also* carry out broader forms of impact assessments in order to:
   a. Concretely substantiate the *specific obligations* laid down in the text (as illustrated by "Risk management layer 2" in Figure 1) and;
   b. Mitigate the *additional risks* for which no specific countermeasure exists in the GDPR (as illustrated in "Risk management layer 3" in Figure 2).

58 I refer the reader to Dewitte (n 3), which traces back the origins of these terms.

3. The combined exercise outlined in point 2 is a form of *Fundamental Rights Impact Assessment* ("FRIA"), a subset of which is covered by a *GDPR Impact Assessment* ("GDPRIA") (as illustrated in Figure 3).

This suggests the existence of different forms of "risk assessment" that vary in scope and complexity (see Figure 4). The broadest would be a *FRIA*, itself the sum of multiple assessments focusing on the impact of the processing of one's personal data on a *specific* fundamental right. This is in line with the conclusions drawn by Karen Yeung and Lee Bygrave in their cross-disciplinary analysis of the Regulation's architecture, in which they argue that "the risk-based approach necessitates that the data controller undertake a contextual 'fundamental rights risk assessment' in order to identify the appropriate level of stringency of the technical and organizational measures that must be adopted to guard against those risks from materializing".[59] While *privacy* ("PIA") and *data protection* ("DPIA") are the usual suspects, the GDPR strives to protect, as discussed above, all data subject's fundamental rights including, for instance, *freedom of expression* ("FoEIA"), *non-discrimination* ("NDIA"), the *right to conduct a business* ("RCBIA") or the *right to an effective remedy a fair trial* ("RERIA"). Or, literally, *any other* fundamental right ("[X]IA"). Building on the role of the GDPR as a "proxy" to mitigate the most pressing risks associated to the processing of personal data for these fundamental rights,[60] performing a *GDPR Impact Assessment* ("GDPRIA")–that is, assessing the degree of compliance of a set of processing operations with the principles and rules it contains, and remedying any deficiency–would lay the groundwork for such a FRIA. While both exercises overlap, the former does not exhaust the latter as controllers will need to complement their compliance efforts depending on the risks inherent to their *specific* activities (layer 2 of Figure 2).

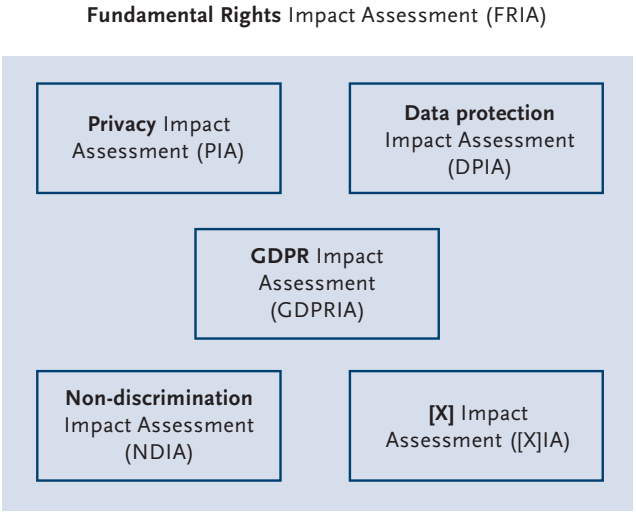

Figure 4. FRIAs, [X]IAs and GDPRIAs

3. A flexible approach to data protection

If the implementation of appropriate technical and organisational measures lies at the heart of data protection by design, controllers must consider a series of criteria when doing so. More specifically, Article 24(1) specifies that account should be taken of "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". Article 25(1) adds "the state of the art" and the "cost of implementation" to the equation. These criteria guarantee the long-term relevance of the Regulation, and leave NSAs and Court the breathing room necessary to adapt to a wide variety of scenarios.

59 Karen Yeung and Lee A Bygrave, 'Demystifying the Modernised European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 Regulation & Governance 137, 146–147 <https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12401> accessed 10 March 2024.

60 The EDPS pitched the same idea in European Data Protection Supervisor (n 1) para 61, if with a slightly different meaning, when it stated that "the GDPR looks at [the general principles of Article 5] as goals to achieve, used as 'proxies' to protect individuals' fundamental rights and freedoms, independently of the level of risk".

3.1 The state of the art

The first element controllers must take into account is "the state of the art". Ad discussed in the first paper, it is worth pointing that the Council deleted the reference to that criterion in the final version of Article 24(1) GDPR.[61] As a result, it only appears in Articles 25(1) and 32(1). The Council also discarded the mention of "current technical knowledge" and "international best practices". Most likely to make that concept as neutral and malleable as possible.

3.1.1 The notion of "state of the art"

The use of the term "state of the art" in an EU legal instrument dates back to 1985, when it was introduced in Article 7(e) of the Product Liability Directive to allow producers to escape the strict liability regime of Article 1 provided that they proved "that the state of scientific and technical knowledge at the time when [they] put the product into circulation was not such as to enable the existence of the defect to be discovered".[62] As rightly pointed out by the European Commission when proposing a new Directive on liability for defective products, "assessing the state of scientific knowledge at the moment of putting [the product] into circulation fails to take account of the fact that producers retain control over digital products beyond that moment and therefore have the means to address defects that become discoverable".[63] It therefore proposed to extend the temporal scope of that exemption to include "the period in which the product was within the manufacturer's control", *de facto* limiting the possibility for manufacturers of–mostly–digital products to "release and forget".[64] The concept of "state of the art" also echoes that of "Best Available Techniques" introduced in Directive 84/360 to combat air pollution.[65] The inclusion of the "state of the art" in the GDPR pursues the same objective, i.e., forcing controllers to constantly monitor scientific progress to identify and incorporate the most up-to-date solutions as part of their countermeasures.

Understanding what is and is not part of the state of the art is critical in delimiting what controllers have to keep track of and potentially implement in their own systems. The EDPB underlines that "existing and recognized frameworks, standards, certifications, codes of conduct, etc. in different fields may play a role in indicating the current 'state of the art' within the given field of use".[66] The IT Security Association Germany (TeleTrust) goes one step further and builds on the 1978 German Federal Constitutional Court's decision in the *Kalkar* decision to distinguish between "Existing Scientific Knowledge and Research" ("ESKaR"),

61 In an attempt to curb the amount of footnotes, the text of the Commission's original proposal, the Parliament's position at first reading, and the Council's position at first reading in this paper are only referenced in full here, but used consistently throughout the text. See, respectively, 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> accessed 10 March 2024; 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 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> accessed 10 March 2024; 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> accessed 10 March 2024.

62 Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the member states concerning liability for defective products, OJ 1985 L210/29.

63 European Commission, 'Impact Assessment Report Accompanying the Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products' <https://single-market-economy.ec.europa.eu/system/files/2022-09/SWD_2022_316_1_EN_impact_assessment_part1_v2.pdf> accessed 11 March 2024.

64 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, COM(2022) 495 Final - 2022/0032 (COD)' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495> accessed 10 March 2024, Article 10(e).

65 Directive 84/360/EEC of 28 June 1984 on the combating of air pollution from industrial plants OJ 1984 L188/20.

66 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 22.

the "State of the Art" ("SotA") and "Generally Accepted Rules of Technology" ("GART") (see Figure 5).[67] Measures included in the ESKaR, states TeleTrust, are "highly dynamic in their development and pass into the 'state of the art' stage when they reach market maturity". The SotA can then be understood as "the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives". Finally, GART include measures "that have been proven in practice and are often described in standards" but for which "the degree of innovation is diminishing". While controllers are not required to consider every new entry to the ESKaR, they must nonetheless go beyond simply updating the measures they have already in place and consider newer alternatives that have been introduced on the market *and* proven efficient. Sticking to GART would have allowed courts to "limit themselves to ascertaining the majority opinion among [practitioners]", which "has the disadvantage of lagging behind developing technology".[68]

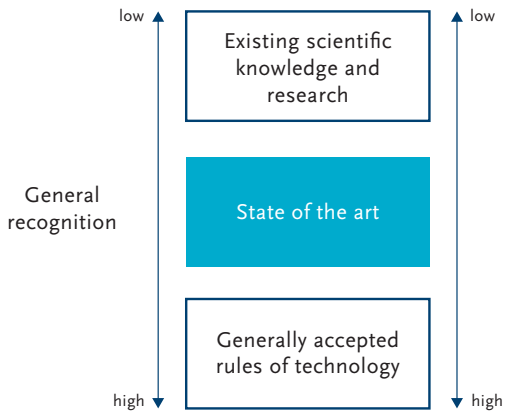

Figure 5. Three-step theory according to the Kalkar decision

NSAs have abundantly referred to guidance documents issued by the ISO, ENISA, and the National Institute for Standards and Technology ("NIST") to illustrate the type of contribution they expected controllers to take into account as part of their SotA assessment.[69] Unsurprisingly, standards from the ISO/IEC 27*xxx* and ISO/IEC 291*xx* families are often used as references when it comes to security measures, and ISO/IEC 31000 as an authoritative source on risk management. ENISA's guidelines on the security of personal data processing also appear among the documents cited,[70] just like NIST's Special Publication 800-63B providing guidelines on digital identity.[71] NSAs have already fined controllers for failing to adequately consider the state of the art

67 TeleTrust and European Union Agency for Cybersecurity, 'IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the Art" - Technical and Organisational Measures' (TeleTrust 2021) Report 11–12 <https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf> accessed 12 March 2024.

68 *Kalkar I* [1978] Entscheidungen der amtlichen Sammlung (BVerfGE) <https://www.servat.unibe.ch/dfr/bv049089.html> accessed 12 March 2024. The Court notes that "[One way to] avoid this drawback [is] to refer [instead] to the 'state of the art' which does not require general recognition and practical confirmation but makes it more difficult for courts and agencies to establish and assess relevant facts".

69 See, more specifically, decision IN 18-11-5 from the DPC (para 74), decisions 56/2021 (para 77), 15/2021 (para 111), 82/2020 (para 129) and 22/2020 (para 26) from the APD, decisions DKN.5130.2215.2020 (p. 13), DKN.5112.1.2020 (pp. 15-16) and ZSPR.421.2.2019 from the UODO (pp. 11-12), and decision 11.17.001.008.029 from the HDPA (points 2.7.2 and 3.4.2).

70 European Union Agency for Cybersecurity, 'Guidelines for SMEs on the Security of Personal Data Processing' <https://data.europa.eu/doi/10.2824/867415> accessed 12 March 2024. See also, for practical use cases applying the former: European Union Agency for Cybersecurity, 'Handbook on Security of Personal Data Processing' <https://data.europa.eu/doi/10.2824/569768> accessed 12 March 2024.

71 Paul A Grassi and others, 'Digital Identity Guidelines: Authentication and Lifecycle Management' (National Institute of Standards and Technology 2017) NIST SP 800-63b <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf> accessed 12 March 2024.

when implementing measures designed to guarantee an appropriate level of security. In decision 9698724, the Garante stated that "applying the MD5 hash function, referred to as 'one-way encryption', for the 'anonymisation' of data, is unreliable as it easily allows detection and correlation, which are two of the main risks of such techniques" (pp. 8-9). In decision 2021-441-10244, the Datatilsynet reprimanded an insurance company for using an archiving system that allowed customers to access all the documents identified using the same claim number, including those sent by the counterparties. In that case, the Datatilsynet noted that "the development of portal solutions providing access to stored documents containing personal data cannot be said to reflect the current technical level if the mail domain suffix is given weight in isolation when allocating access". It then underlined that "it would normally be part of the current technical level that built-in follow-up checks ensure that such an automated process only provides correct accesses" (p. 4).

3.1.2 Assessing the "state of the art"

Controllers are free to select the method to assess the state of the art, as long as they *properly document it*. The DPC made that clear in its decision IN 21-4-2 against Meta Platform Ireland Limited. After noting that Meta "failed to provide any documentation to show its analysis of the state of the art" (para 131), the Irish regulator performed its own assessment to conclude that the rate limiting and bot detection measures set up by the platform were not appropriate to prevent the scraping of contact information in a world where "captchas" and "post-incident analyses" could have been implemented (paras 140-149). The Rechtbank Midden-Nederland held a similar reasoning in its interlocutory ruling AWB - 19 _ 1687, in which a data subject successfully exercised his right to rectify his medical file, but complained that the modification took the form of an annex, rather than of an alteration of the original document. This, he argued, could mislead the persons authorised to access his medical file should they not bother to browse through all the documents. The Dutch Employee Insurance Schemes Body ("UWV") investigated various technical solutions to make that modification more apparent, but considered them all "not technically feasible" (para 13.1). The Court found that the UWV did "not sufficiently substantiate what research was conducted and what that research consisted of" to support its conclusion since the SotA assessment only contained "a brief summary of the results of the research, but [did] not reflect or provide insight into the research itself" (paras 13.3).

Yet, specific guidance exists on how to perform that assessment. Of particular relevance is the methodology developed by ENISA to assess the maturity of PETs by combining their technology readiness and their privacy enhancing quality.[72] Taking inspiration from NASA's TRL measurement, ENISA proposed its own scale ranging from "idea" to "research", "proof of concept", "pilot", "product" and "outdated". Similarly, it built on the eight quality characteristics of software and systems elicited in ISO/IEC 25010 to come up with its own quality scale comprising the following nine elements, each assigned a weight reflecting their importance. When combined, ENISA's readiness and quality scales can express various degrees of "PET Maturity" (see Figure 6). In turn, determining the "readiness" and "quality" level of a given PET requires selecting a board of experts and gathering both "measurable indicators" and "expert opinions" through questionnaires. TeleTrust has developed a similar method to assess the degree of recognition of certain technologies as well as their effectiveness. That approach, aims "to provide companies using it and providers (manufacturers, service providers) alike with assistance in determining the 'state of the art' within the meaning of the IT Security Act and the General Data Protection Regulation".[73]

72 Marit Hansen, Jaap-Henk Hoepman and Meiko Jensen, 'Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies - Methodology, Pilot Assessment, and Continuity Plan' (European Union Agency for Cybersecurity (ENISA) 2015) Report <http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215974:EN:HTML> accessed 15 March 2024.

73 As such, states TeleTrust, "the document can serve as a reference for contractual agreements, procurement procedures or the classification of security measures implemented". TeleTrust and European Union Agency for Cybersecurity (n 67) 6.

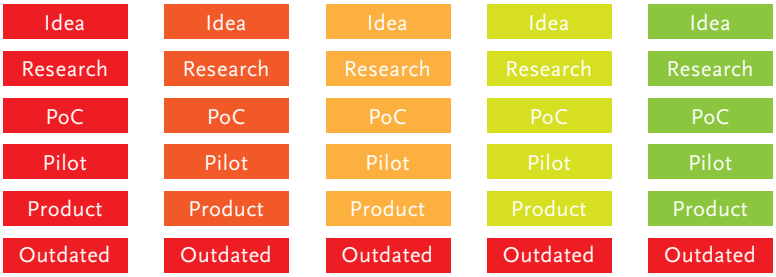

Figure 6. Overview of Possible PET Maturity Level Values

3.1.3 A community approach to the state of the art

It is worth noting that both the methodologies outlined above involve resorting to experts to assess the maturity and adequacy of the measures proposed in scientific contributions or available on the market. That form of "outsourcing" is inherent to the nature of the exercise. Some controllers might, however, not be able to afford it due to a lack of financial resources, in-house knowledge, or both. More worryingly, NSAs, the competences of which include *verifying* that controllers have correctly assessed the state of the art prior to implementing their countermeasures, have also reported a shortage of funding and human resources.[74] The Board is not immune to that phenomenon, as illustrated by its conclusions in Binding Decision 2/2023. Tasked with assessing the appropriateness of the age verification processes implemented by TikTok to bar underage users from accessing the platform, it acknowledged that it "does not have sufficient information, in particular in relation to the state of the art element, to conclusively assess [TikTok's] compliance with Article 25(1) GDPR" (paras 217, 244). Properly assessing the state of the art is, indeed, a time-consuming, resource-heavy task that would benefit from a degree of knowledge pooling.

ENISA pushed that idea forward in its maturity assessment methodology published in 2015, and prototyped an online platform designed to gather experts' opinion on the readiness and quality of selected PETs in a structured and searchable way.[75] This departed from similar initiatives such as the privacypatterns.org and privacypatterns.eu repositories,[76] Ohla Drozd's catalogue of privacy patterns,[77] or the Centre for Data Ethics

74 European Data Protection Board, 'Overview on Resources Made Available by Member States to the Data Protection Supervisory Authorities' (European Data Protection Board, 2022) <https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf> accessed 21 March 2024; The report concludes that "an important majority of SAs [77%, NDLR] explicitly states that they do not have enough [financial] resources" and that "a vast majority of SAs [87%, NDLR] have explicitly stated that they do not have enough human resources". This is also apparent from the answers provided by NSAs in the context of the 2020 evaluation of the GDPR foreseen by Article 97. The individual replies from NSAs are available here: European Data Protection Board, 'Individual Replies from Data Protection Supervisory Authorities' (European Data Protection Board) <https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en> accessed 21 March 2024; See also the contribution of the EDPB to the said evaluation: European Data Protection Board, 'Contribution of the EDPB to the Evaluation of the GDPR under Article 97' (European Data Protection Board, 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf > accessed 21 March 2024.

75 The prototype was presented in September 2016. See: European Union Agency for Cybersecurity, 'Privacy Enhancing Technologies: Evolution and State of the Art' (European Union Agency for Cybersecurity, 2016) <https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art> accessed 21 March 2024.

76 The privacypatterns.org repository is the output of an interdisciplinary research project that received the support of the United States' Department of Homeland Security, NIST, the European Union's Seventh Framework Programme (via the PRIPARE project) and the Berkeley Center for Law and Technology. The privacypatterns.eu repository is a sibling initiative that involved, on top of the EU FP7 PRIPARE project, Patterns4Privacy, privacy wiki, privacypatterns.org and PRIPATS.

77 Olha Drozd, 'Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into the Software Development Process' in David Aspinall and others (eds), *Privacy and Identity Management. Time for a Revolution?*, vol 476 (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-41763-9_9> accessed 21 March 2024; The actual catalogue is available here: <https://privacypatterns.wu.ac.at:8443/catalog/> accessed 21 March 2024.

and Innovation's Privacy Enhancing Technologies Adoption Guide,[78] in that it not only indexed existing solutions, but also provided a systematic framework for their evaluation. In that regard, ENISA's initiative leans more towards a repository of the *state of the art* within the meaning outlined above, rather than a collection of *PETs* strictly speaking. Unfortunately its uptake has been rather low.[79] Despite all the efforts poured into the development of the platform as well as the concrete recommendations put forward by ENISA, the repository has–at least publicly–been discontinued. That is unfortunate, as there exists, to the best of my knowledge, no other alternative that bundles a comparable degree of legal certainty together with a structured peer-review process. A solution at the crossroads between industry, research and regulators such as the platform set up by ENISA would therefore appear–at least on paper–as the most constructive way forward. Yet, there is little incentive to do so. Especially not for the biggest market players who would need to disclose their portfolio of countermeasures to competitors, all the while opening up their compliance programme for scrutiny by regulators and the public.

3.2 The cost of implementation

The second element that controllers must take into account in their data protection by design efforts is the "cost of implementation". Exactly as the "state of the art", that criterion only appears in the final version of Articles 25(1) and 32(1), not in Article 24(1). As exposed in the first paper, the Council got rid of the reference to the "cost of implementation" in Article 24(1). The reason behind that choice is, just like for the "state of the art", nowhere to be found in the preparatory works.

3.2.1 The notion of "cost of implementation"

According to the EDPB, the "cost of implementation" refers to "resources in general, including time and human resources".[80] While that notion is also used in Article 17(2) GDPR to modulate the "reasonable efforts" controllers that have made personal data public must take to inform other controllers that a data subject has requested the erasure of their personal data, guidance is lacking as to what the "cost of implementation" exactly covers and how it should be calculated in practice. More specifically, it is unclear whether it refers to the *gross* or *net* cost of implementation, i.e., whether it should reflect the total amount of resources spent by the controller, or also take the potential benefits gained from implementing a specific measure into consideration. Indeed, implementing any measure is likely to decrease the likelihood and consequences of administrative or judicial proceedings, and the amount of potential sanctions and damages.

The EDPS seems to have positioned itself in favour of calculating the net cost of implementation when it states that "when choosing technical and organisational measures for data protection, or assessing the measures taken by an organisation [...], the benefits organisations enjoy from their investments are balanced against the costs".[81] Since factoring these benefits in the calculation of the cost of implementation will inevitably lower the final figure, doing so will also affect the outcome of the proportionality assessment by tipping the scale in favour of the implementation of measures that might, at first sight, have appeared too expensive with regard to their added value. Illustrating the above, Selzer et al. have proposed a method to evaluate the cost of implementing state of the art security countermeasures based on interviews with representatives of 27 organisations of varying sizes and from different industries, and come up with detailed cost tables for the most represented technical and organisational solutions pursuant to Article 32 GDPR.[82]

78 The Adoption Guide is structured around a question-based flowchart designed to help decision-makers in selecting appropriate PETs, and is accompanied by a repository of use cases that showcases examples of actual solutions that have been deployed in practice to overcome privacy challenges. The repository is available here: Centre for Data Ethics and Innovation, 'PETs Adoption Guide Repository' (Centre for Data Ethics and Innovation) <https://cdeiuk.github.io/pets-adoption-guide/repository> accessed 21 March 2024.

79 European Union Agency for Cybersecurity, 'ENISA's PETs Maturity Assessment Repository - Populating the Platform' (European Union Agency for Cybersecurity) <https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository> accessed 21 March 2024.

80 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 23.

81 European Data Protection Supervisor (n 1) para 95.

82 A Selzer, D Woods and R Böhme, 'An Economic Analysis of Appropriateness under Article 32 GDPR' (2021) 7 European Data Protection Law Review 456, 459–460 <http://edpl.lexxion.eu/article/EDPL/2021/3/15> accessed 21 March 2024. The detailed cost tables are available here: <https://www.sit.fraunhofer.de/edpl-annex-cost-table/> accessed 21 March 2024.

3.2.2 The role of the "cost of implementation"

While uncertainty remains as to the method that should be used to calculate the "cost of implementation", the role it plays in the risk-based approach is clearer. As pointed out by the EDPB, controllers do not have to spend "a *disproportionate* amount of resources when alternatives, less resource-demanding, *yet effective* measures exist" (emphasis added).[83] The Board does not, however, detail what the "cost of implementation" should be weighed against in that proportionality assessment. One could extrapolate that the amount of money controllers are expected to spend on the implementation of a specific measure must be proportionate to the risk for data subject's rights and freedoms that the said measure aims to mitigate. This will require controllers to first identify the risks raised by its processing operations, then map the state of the art with regard to relevant mitigation strategies, and finally select the most appropriate measures depending on the importance of the asset to be protected. Deploying a software on company laptops to monitor employees' performance at work raises, for instance, significantly more risks than, say, relying on a solution based on keeping track of check-ins and check-outs through card readers. While, in both cases, the controller is expected to implement *effective* measures to ensure, for instance, the transparency of the underlying personal data processing, their cost will be less of a limiting factor in the former case than in the latter.

It is also crucial to note that the measures controllers are required to implement must be *appropriate* to address the risks identified *regardless* of their cost of implementation. The "cost of implementation" can certainly orient the choice between measures that provide sufficient guarantees, but can never justify opting for a solution that does not meet the "appropriateness threshold" as detailed earlier in this paper (see Figure 7). In other words, if the only countermeasure that adequately mitigates a specific risk also proves to be very expensive, the controller will have no choice but to implement it anyway. The likelihood and severity of the risks at stake–and, if considering the risk of non-compliance as the main threat for controllers to mitigate, the importance of the corresponding legal requirement–only influence the relevance of the cost factor when selecting *among* appropriate measures; the higher the risk–or the more important the provision–the less constraining the cost of implementation. The asset to be protected is not the controller's finances, but the data subjects' rights and freedoms with regard to the processing of their personal data.

There will be situations where an objectively better solution (green dot in Figure 7) is also less expensive than an alternative of lesser quality (red dot in Figure 7). Or where two or more measures are equally good, but differ when it comes to the cost of their implementation. In these cases, controllers are rightfully expected to opt for the cheapest measure, provided that it is the best option within their respective price bracket. But there will also be scenarios where controllers have to decide whether to implement an objectively better but more expensive measure (orange dot in Figure 7). In that case, the substance of the risk to be mitigated and the importance of the corresponding fundamental right will determine the "weight" of the "cost of implementation" (see Figure 7) in the selection process. It is therefore not unrealistic that a particularly risky processing operation requires controllers to shell out a significant amount of money for a marginal quality increase.

Lina Jasmontaite seems to suggest – though maybe incidentally – that the cost of implementation should be proportionate "to the controllers' *available resources*" (emphasis added).[84] This also transpires from the ICO guidance on Article 25(1) GDPR, which advises controllers that "how you go about doing [data protection by design] depends on your circumstances–who you are, what you are doing, *the resources you have available*, and the nature of the data you process" (emphasis added).[85] I have some reservations as to the relevance of that criterion. First, it is nowhere to be found in the text of the GDPR, nor in any of the relevant national or European soft law instruments but that of the UK regulator. The closest reference to that concept is in Recital 81, which complements Article 28 and states that "when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and *resources*, to implement technical and organisational measures which

83 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 24.

84 Jasmontaite and others (n 23) 178. The author does not mention the reasoning behind the inclusion of that criterion.

85 Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' 216 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> accessed 17 march 2024.

will meet the requirements of this Regulation" (emphasis added). Yet, a closer look at the wording of Recital 81 suggests that the "resources" available to processors only influence the selection of the entity to which controllers will delegate part of their processing activities, *not* that of the appropriate measures to be implemented.

Second, none of the decisions analysed as part of the case law review described in Figure 6 refers to the resources available to the controller as a limiting factor when it comes to the implementation of appropriate technical and organisational measures. At most, the DPC left some ambiguous statements on the role of that criterion in its decision IN 21-4-2 issued against Meta Platforms Ireland Ltd. More specifically, it noted that "the examples of measures provided above [i.e., preventing exact matches between profiles and phone numbers, implementing rate limits and setting-up 'captchas'] were all viable existing measures at the time of the Temporal Scope, some of which [Meta] has indeed subsequently implemented, which would seem to show that the cost of implementation would not have posed an issue to [Meta]" (para 154). While this clearly implies that Meta had enough money to implement all the measures detailed above, the Irish regulator did not explicitly state that lower financial resources would have exempted the company from doing so.

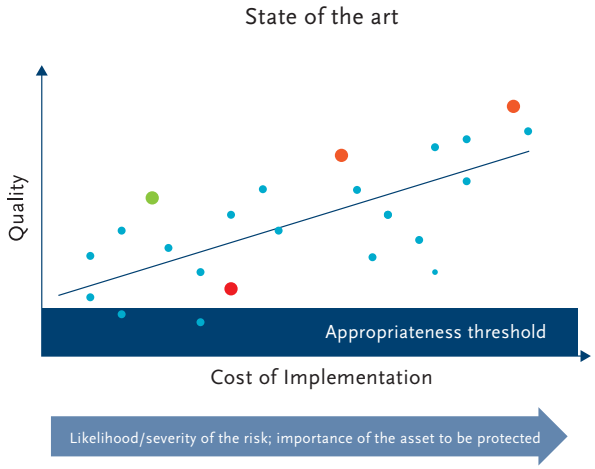

Figure 7. Role of the cost of implementation on the selection process

Lastly, considering the resources available to the controller alongside the risks raised by the processing when evaluating the influence of the "cost of implementation" on the measures to be implemented would, I argue, run contrary to the very objective of Articles 24(1) and 25(1) GDPR, i.e., ensure that each of these risks is *appropriately* mitigated. Adding a factor of economic viability to the cost-specific proportionality assessment would allow controllers to hide behind the lack of sufficient resources to justify the absence of proper countermeasures. This would mean that a new entrant that engages in particularly risky processing activities, but does not have the financial resources to set up a proper risk management strategy, would be able to get away with a more limited compliance exercise. Instead, at equal risks, a wealthier controller, I argue, should be required to go the extra mile and implement a more expensive measure, even though the increase in protection for data subjects' rights and freedoms is only marginal. But a controller that has limited resources at its disposal cannot use its financial situation to support the implementation of measures that do not appropriately address these risks.

3.2.3 The "cost of implementation" and deterrence

The "cost of implementation" also plays a role in the calculation of the fine NSAs can impose following a breach of data protection by design. The APD emphasised that point early on in its decision 42/2020 issued against the Belgian telecom operator Proximus, which eventually led to case C-129-21.[86] Having noted that

86 *Proximus NV v Gegevensbeschermingsautoriteit*, Case C-129/21 [2022] Electronic Reports of Cases (ECLI:EU:C:2022:833).

acting upon the data subject's withdrawal of consent to have their personal data published in Proximus' telephone directory and informing third parties recipients of the said withdrawal would require the company to make "necessary investments", the Belgian regulator underlined the possibility that, "in case of too light sanctioning", Proximus might simply "accept the risk of being subjected in the future to decisions finding infringements with limited sanctioning". "This", rightfully added the APD, "would mean that infringements could continue to occur not only in this but also in other cases concerning compliance with the provisions of the GDPR" (para 131).

This ties back to the requirement for administrative fines to be "dissuasive" (Article 83(1) GDPR). In the words of the EDPB, a fine is dissuasive if it "has a genuine deterrent effect"; in turn, deterrence is achieved "where [the fine] prevents an individual from infringing the objectives pursued and rules laid down by Union law", based "not only the nature and level of the fine but also the likelihood of it being imposed".[87] That premise should be combined with basic economic theory, according to which a rational economic actor such a controller will, when confronted with a choice, naturally perform a cost-benefit analysis to determine its best course of action.[88] When it comes to compliance with data protection law, the controller will then inevitably compare the cost of implementing the measures required by Articles 24(1) and 25(1) GDPR (i.e., the cost of compliance) with the costs associated to judicial and/or administrative proceedings in case it decides not to do so, including the likelihood and level of a potential fine as well as the bad press that goes along with it (i.e., the cost of non-compliance).[89] In order for the fine to be "dissuasive", the cost of non-compliance must be higher than the cost of compliance.[90] The "cost of implementation" within the meaning of Article 25(1) GDPR is therefore a crucial factor for NSAs to calculate the amount of a "dissuasive" fine for a breach of data protection by design since it represents the threshold below which controllers, acting as rational entities, might simply decide to tolerate the risk associated with non-compliance.[91]

3.3 The nature, scope context and purposes

Next to the "state of the art" and the "cost of implementation", controllers must also consider the "nature, scope, context and purposes" of their processing activities when selecting appropriate countermeasures. Absent from the European Commission's original proposal, these four elements were, as noted in the first paper, added by the Parliament in Article 24(1), and by the Council in Article 25(1). Most likely to prevent any such discrepancy from watering down the scope of the risk-based approach.

3.3.1 The "nature" of the processing

The "nature" of the processing, states the EDPB, should be understood as the "inherent characteristics of the processing".[92] This concept, argues Lina Jasmontaite, should be distinguished from the nature of the *personal data* processed, i.e., their qualification as regular or special categories of personal data.[93] Instead, it refers to the intrinsic features of the processing such as, for instance, its degree of automation and

87 European Data Protection Board, 'Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR' paras 142–143 <https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf> accessed 21 March 2024, quoting *Commission of the European communities v French republic*, Case C-177/04, Opinion of Advocate General Geelhoed [2005] I ECR 06263 (ECLI:EU:C:2005:717) para 39. The Advocate General interpreted "effectiveness" within the meaning of Regulation 2847/93 as "meaning that there is a credible probability that, in case of non-compliance, fishermen will be running a high risk of being detected and of sanctions being imposed which would at least deprive them of any economic benefit accruing from the transgression of the fisheries provisions".

88 Lawrence E Blume and David Easley, 'Rationality' in Palgrave Macmillan (ed), *The New Palgrave Dictionary of Economics* (Palgrave Macmillan UK 2008) 3 <https://link.springer.com/10.1057/978-1-349-95121-5_2138-1> accessed 21 March 2024.

89 Mitchell Polinsky and Steven Shavell, 'The Theory of Public Enforcement of Law', *Handbook of Law and Economics* (Elsevier 2007) 413 <https://linkinghub.elsevier.com/retrieve/pii/S1574073007010067> accessed 21 March 2024.

90 As noted, if under EU antitrust law, by Wouter P.J Wils, 'Optimal Antitrust Fines: Theory and Practice' (2006) 29 World Competition 29 <https://kluwerlawonline.com/journalarticle/World+Competition/29.2/WOCO2006014> accessed 21 March 2024.

91 Hazel Grant and Hannah Crowther, 'How Effective Are Fines in Enforcing Privacy?' in David Wright and Paul De Hert (eds), *Enforcing Privacy*, vol 25 (Springer International Publishing 2016) 304 <http://link.springer.com/10.1007/978-3-319-25047-2_13> accessed 23 March 2024, observe that "fines would appear to be at their most effective in cases where there has been an element of choice on the part of the data controller, which then led to a breach".

92 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 28.

93 Jasmontaite and others (n 23) 178.

human involvement, its repetitive or intrusive character, the amount of recipients–third parties or not– and the existence of transfers to third countries. The Irish DPC seems to have vouched for that reading in decisions IN 21-4-2 and IN 20-7-4, which both explicitly refer to the "nature" of the processing as the "basic or inherent features of the operations performed on personal data" (paras 58 and 230, respectively).

In decision NAIH-85-3/2022, the Hungarian regulator fined Budapest Bank for the use of a speech recognition software to assess customers' emotions, and noted that "[t]he analysis, use and storage of the voice and emotional state of data subjects is considered to be a processing of a *sensitive nature*" (emphasis added, para 44). "The operating principle of AI", it added, "is generally difficult to understand", which "is one of the reasons why the use of artificial intelligence in data processing requires particular care if the controller wants to comply with transparency and accountability" (para 80). The Norwegian Datatilsynet considered that imposing the use of Strava to verify whether students had completed their sport assignments was particularly invasive, as this would entail the processing of their location data and pave the way for the systematic monitoring and comparison of their sport performance (decision 20/02147-6, p. 3). Other examples of particularly sensitive processing activities include the automatic forwarding of employees' emails (decisions 21/01164 and 20/02274), credit assessment (decisions 20/04401-11 and IN 19-7-2) and the use of surveillance cameras at the workplace (decision 20/01874).

It is worth noting that the "nature, scope or purpose" of the processing also plays a role in determining the amount of administrative fines as per Article 83(2)a GDPR. Some wording oddities aside,[94] these concepts bear the exact same meaning as in Articles 24(1) and 25(1). This makes the jurisprudence dealing with the imposition of administrative fines particularly relevant to understand what these notions exactly cover, as assessing the "nature", "scope" and "purpose" of the processing is a prerequisite to decide whether to impose such as fine, as well as its amount. When it comes to the "nature" of the processing, the EDPB noted, in its Binding Decision 01/2020 concerning a case brought against Twitter before the Irish DPC, that "one must also take into consideration the fact that the 'processing concerned' involved communications by data subjects who *deliberately chose* to restrict the audience of those communications" (para 186, emphasis added). As a result, concluded the EDPB, a bug that resulted in certain private "Tweets" becoming public following a change of email address on Android device is all the more serious given that many users will have specifically relied on that functionality to "share information or views in the comfort of what they believe to be a private and controlled environment".[95] In this particular case, the contrast between the restricted nature of the processing and the consequences of the infringements attributable to Twitter played a pivotal role in the decision to impose a 450,000 euros fine in decision IN-1-1.

3.3.2 The "scope" of the processing

The "scope" of the processing is more straightforward than its "nature", and simply refers to its "size and range".[96] In other words, the amount of personal data being processed. Controllers, however, might not always be in a position to precisely delineate the extent of their processing operations. This might be the case when developing a new service, or bringing an existing one to new markets. Yet ignorance, however genuine, is not an excuse for leaving that criterion aside. Such is the view expressed by the Belgian APD in decision 48/2022. Confronted to the question as to whether Brussels Airport should have conducted a DPIA before rolling-out thermal cameras amidst the COVID-19 pandemic, the APD noted that "it had to be considered that *all* screened passengers could be affected by the processing *even if* the airport ignored the percentage of passengers that would have a body temperature superior to 38°C" (emphasis added, para 186).

The notion of "large-scale processing" within the meaning of Article 35(3)b and c GDPR provides valuable insights on the elements that must be factored in the assessment of the "scope" of the processing in the context of Articles 24(1) and 25(1). According to Recital 91 GDPR, these include the processing that

94 These being the absence of the "context" compared to the wording of Articles 24(1) and 25(1) GDPR, the shift from a cumulative ("and") to an alternative ("or") coordinating conjunction, and the omission of a comma between "nature" and "scope".

95 The DPC originally included that argument in its draft decision, but decided to give it more weight as part of its assessment of the criteria under Article 83(2), as recommended by the EDPB in its Binding Decision 01/2020. See para 14.4 of decision IN-19-1-1.

96 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 28.

involve "a considerable amount of personal data at regional, national or supranational level". The list of criteria compiled by the WP29 to determine whether a specific processing is carried out on a "large scale" also provides a solid baseline to assess the overall "scope" of any type of processing.[97] In its Minister van Buitenlandse Zaken decision, the Dutch Autoriteitpersoonsgegevens concluded that the administration had not implemented adequate security measures when processing the personal data of visa applicants, and justified a 565,000 euros fine by referring to the very large number of data subjects concerned (para 222). The Finnish regulator also relied on quantitative findings when fining Otavamedia in case 6097/161/21, noting that the controller was a large Finnish media company the audience of which comprised more than 2.3 million active readers per month (p. 35). The "scope" element also played a particularly important role in assessing the appropriateness of the measures implemented by telecommunication operators, as these actors naturally process personal data from millions of subscribers. This is notably the case in Decision of 21 July 2022 (p. 2), ΑΠΟΦΑΣΗ 4/2022 (p. 43), SAN-2021-021 (para 114), NAIH-924-10/2021 (p. 14) and PS/00059/2020 (p. 91).

It is also crucial to distinguish the "scope" of the *processing* and the "scope" of a *personal data breach* as defined by Article 4(12) GDPR. While the latter exclusively serves as a yardstick to determine the level of an administrative fine as per Article 83(2)a GDPR, the former influences *both* the selection of the countermeasures *and* the amount of the fine. This calls for two remarks. First, the scope of a personal data breach does not have any influence on the type of measures that controllers must implement as per their obligations under data protection by design. This is logical, given that such risk assessment must be carried out at the time of the determination of the means for processing, and therefore *before* any such breach could even materialise itself. Second, and considering a personal data breach that affects an equal number of data subjects, a controller that processes vast amounts of personal data should incur a more severe fine than a controller that processes a more limited dataset. The EDPB hammered on the importance to correctly assess the "scope" of the processing when determining the amount of an administrative fine in its Binding Decision 01/2020, in which it noted that that Irish DPC, in its draft decision, "substitute[s] the scope of the processing with the number of the data subjects affected". According to the Board, "the scope of the 'processing' to take into consideration in the determination of the fine is not the processing operation consisting in the (accidental) disclosure (personal data breach), or the cause thereof, but rather the scope of the underlying processing carried out by [Twitter]" (para 187).[98]

3.3.3 The "context" of the processing

The "context" of the processing, states the EDPB, "refers to circumstances of the processing, which may influence the expectations of the data subject".[99] As noted by the WP29 in its Guidelines on purpose limitation, "the nature of the relationship between the controller and the data subject" is an integral part of that "context".[100] So are power and information asymmetries. The processing of personal data in an employment context, for instance, is particularly sensitive and requires the implementation of specific safeguards that account for the subordination relationship between the employer and the employee. There is no shortage of case law on the matter. In its decision PVN-2021-13 concerning the installation of surveillance cameras in a restaurant, the Personvernnemnda considered that such processing concerned

97 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' 9 <https://ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 25 March 2024.

98 It is worth noting that the DPC, in its final decision IN-19-1-1, does not seem to have integrated that distinction. Indeed, the Commissioner merely notes the following, right before acknowledging the comments formulated by the EDPB on the "scope" of the processing: "In terms of the *scope* of the processing, [Twitter] has confirmed to the Commission that, as far as it can identify, between 5 September 2017 and 11 January 2019, 88,726 EU/ EEA users were affected by this bug. However, [Twitter] has further confirmed that it dates the bug to 4 November 2014, but that it can only identify users affected from 5 September 2017. In this regard, [Twitter] has confirmed its belief that 'additional people were affected during the period from 4 November 2014 to 14 January 2019 when the bug was fully remediated'" (emphasis in original). By focusing on the data subjects affected by the bug, rather than on the scope of the underlying processing operations as a whole, the DPC therefore seems to omit a crucial element when assessing the amount of the fine.

99 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 28. See also Jasmontaite and others (n 23) 179.

100 Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' 31 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 24 March 2024.

"employees who are in a special relationship of dependence with their employer", and adjusted the amount of the fine accordingly as per Article 83(2)g (p. 7). The Belgian APD came to a similar conclusion in decision 72/2020 regarding the processing, by an employer, of its employees' trade union data which it could, at least in theory, use to "put pressure on workers or discriminate against them, particularly during promotion procedures" (para 50).

Supervisory authorities also tend to consider that personal data processed in a medical context deserve a higher degree of protection. The Tietosuojavaltuutetun acknowledged that in decision 1150/161/2021, in which it underlined that "the confidentiality of the treatment relationship and the protection of the patient's privacy are of particular importance in the provision of psychotherapy services" (p. 30). The Finnish regulator used that argument as an aggravating factor when determining the amount of the fine issued against Psykoterapiakeskus Vastaamo Oy for various security breaches, which it eventually set at 608,000 euros. So did the Belgian APD in decision 117/2021 when assessing the appropriateness of the security measures implemented by a hospital to secure the sending of forms that could contain special categories of personal data (paras 35-36). In its decision DI-2019-3840 issued against Sahlgrenska University for a lack of adequate access control measures, the Swedish Datainspektionen also noted that "patient[s] are dependent on receiving care and [are] therefore in a vulnerable situation" (p. 31).

Education is also a context that calls for a thorough risk assessment and mitigation process, mostly given the age of the data subjects and the lack of viable alternative. This is especially true when such processing involves the use of new and complex technologies, as highlighted by the Datatilsynet in its decision 2020-431-0061 (2) issued against the Helsingør Municipality for failing to adequately assess and documents the risks inherent to the use of Google Chromebooks and Google Workspace. The reasoning of the Datatilsynet is particularly interesting in that it considers the broader ecosystem in which Google–the provider of both the hardware and the software used by pupils in the above-mentioned case–operates to justify why the countermeasures implemented by the Municipality fail to meet the threshold of Articles 5(2) GDPR. More specifically, the Danish regulator boldly notes that "the technologies used to deliver and support the selected service are also used to deliver other parts of Google's products", and that "these are used for information collection, targeted marketing and the sale of this information" (p. 11). In other words, while the processing of pupils' personal data in an educational context *already* raises bar for the risk assessment, the fact that these activities are carried out by an actor that also pursues advertising and analytics purposes calls for the implementation of even stronger countermeasures.

The status of the controller, such as its position on the market, is also relevant when assessing the impact of the processing.[101] Formulated in the context of Article 6(1)f GDPR, that observation also contributes to shaping the overall "context" of the processing operations. Supervisory authorities seem to have given more weight to that factor when confronted to former monopolies such as incumbent local exchange carriers[102] or natural gas and electricity suppliers.[103] These long-established companies are indeed expected to lead by example.[104] Of particular relevance is the finding of the Garante in decision 9735672, stating that the mechanisms put in place by Enel Energia to verify the lawfulness of promotional calls made by partners outside its official networks were insufficient in light of its "history, structure and organisational size", which "would have allowed the company, a leader in the Italian energy market and a long-standing protagonist of the economic-productive life of the country to implement cutting-edge organisational measures for the

101 Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' 40–41 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 21 March 2024.

102 The following cases are worth a mention: AZOP's Decision of 21 July 2022 against A1 Hrvatska (p. 2), CNIL's decision SAN-2021-021 against Free Mobile (para 114), AEPD's decision PS/00059/2020 against Vodafone España (pp. 90-91), and APD's decision 42/2020 against Proximus.

103 See, more specifically the Garante's decision 9735672 issued against Enel Energia and the AEPD's decision PS/00236/2020 which imposed a 1,500,000 euros fine on EDP Energia.

104 Illustrating the above, the APD for instance noted in decision 42/2020 that "[a]s a major player in the telecommunications sector, [Proximus] has an exemplary role, and should organise its technical and organisational measures in such a way that the provisions of the GDPR and the national implementing regulations can be duly complied with" (para 123).

protection of data subjects" (p. 24). Supervisory authorities have reached similar conclusions when it comes to controllers acting as public authorities or public figures.[105]

It should also be noted that the fact that the processing operations have been set up in an emergency context does not in any way diminish the controller's duty to implement the necessary measures to comply with the provisions of the Regulation. So was the opinion expressed amidst the COVID-19 pandemic by the Belgian APD in decision 48/2022 concerning the installation of thermal cameras at Brussels Airport (paras 21, 123), by the Garante in decision 9556958 concerning the processing of food aid applicants' personal data by the Municipality of Palermo (pp. 6, 9) and by the Datatilsynet in decision 20/02147-6 concerning the use of Strava by teachers in the Ålesund Municipality to remotely monitor students' progress with their physical education homework (p. 2).

3.3.4 The "purposes" of the processing

Lastly, the "purposes" of the processing refer to the "aim" of the processing.[106] In other words, to "why the processing is taking place.[107] That element is intrinsically linked to "purpose specification", the first component of the "purpose limitation" principle enshrined in Article 5(1)b GDPR. Certain purposes benefit from a specific regime. The processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is subject to an entirely different legal instrument, namely Directive 2016/680.[108] Further processing for scientific research purposes are presumed compatible with the purposes for which the personal data were originally collected, provided that the controller has implemented "appropriate safeguards for the rights and freedoms of data subjects" GDPR (Article 5(1)b, second part). The GDPR also provides for a more flexible retention period (Article 5(1)e, second part), a lighter transparency regime (Article 14(5)b), as well as derogations from certain data subject's rights (Articles 17(3)d and 89(2)). Processing biometric data with the view of uniquely identifying or authenticating a natural person, on the other hand, triggers the applicability of the general prohibition of Article 9(1) GDPR. Bottom line being, since the GDPR pairs certain purposes with specific legal requirements, these purposes will inevitably influence the types of measures that controllers must implement as part of their data protection by design obligations.

Building on the narrative developed in Section 2.3, these "riskier" purposes influence how controllers are expected to mitigate the associated risks, either when substantiating the requirements explicitly contained in the Regulation–i.e., layer 2 in Figure 1–or when contemplating the implementation of measures that the legislator has not foreseen–i.e., layer 3 in Figure 2. The processing of health-related personal data through a smartwatch, for instance, raises different risks depending on whether it merely aims to provide users with a way to track their performance, or whether it also serves as a baseline to determine the amount of a premium in the context of a partnership with an insurance company. In turn, the said purpose directly impacts how the (joint) controller(s) must comply with their respective transparency obligations. If a simpler privacy policy might do the trick in the former case, tailoring an insurance premium based on special categories of personal data requires a thorough but intelligible explanation of, among other elements, the logic and consequences of such processing, as this lead to discriminating people who do not have enough time to dedicate to physical activities.

105 See the Autoriteitpersoonsgegevens's decision in Minister van Buitenlandse Zaken (para 224), the Garante's decision in 9556958 (pp. 12, 20) and the APD's decision in 54/2020 (para 30).

106 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 28.

107 European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' para 35 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en> accessed 22 March 2024.

108 Directive 2016/680/EU 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 2016 OJ [2016] L 119/89.

Next to the purposes specifically mentioned in the GDPR, supervisory authorities have also progressively identified certain purposes which, considering the risk they pose for data subject's fundamental rights, call for stricter countermeasures. The Datatilsynet has repeatedly emphasised that the processing of personal data for credit assessment purposes is "intrusive" and "constitutes a major interference with individuals' right to privacy".[109] In decision 21/02293-10, the Norwegian authority therefore took that element into account, under Article 83(2)d GDPR, when issuing a 200,000 NOK fine against Recover AS for the lack of appropriate internal procedures and process which led the company to credit assess the wrong person (para 6.9, d). The NAIH also noted that the use of AI for the purpose of inferring emotions "is highly undesirable and should be prohibited except in certain well-defined use cases". That factor played a decisive role in the Hungarian regulator's decision to impose a 250,000,000 HUF fine against Budapest Bank in case NAIH-85-3/2022 for the use of voice analysis software on recorded customer calls (para 83).

3.4 The risks for the rights and freedoms of natural persons

Last but certainly not least, controllers must tailor their countermeasures to the "risks of varying likelihood and severity for [the] rights and freedoms of natural persons posed by the[ir] processing". As stated in the first paper, the Parliament added that last element to Articles 24(1) and 25(1) in its position at first reading, while the Council introduced the idea of "varying likelihood and severity". That vernacular directly builds on the vocabulary used in risk management, thereby anchoring data protection by design in a long tradition of risk assessment methodologies and frameworks.

3.4.1 Of "risks" to "data subject's rights and freedoms"

As illustrated in Figures 1 and 2, the "risks to data subject's rights and freedoms" play a double role. First, they define the material scope of Article 25(1) GDPR which, read in combination with Recital 75 and Article 1(2), comprises *all* data subject's fundamental rights, including but not limited to privacy and data protection, that might be impacted by the processing of their personal data. Second, that criterion is also one of the parameters that controllers must consider when selecting the most "appropriate" countermeasure to mitigate a given risk, either when complying with the provisions explicitly contained in the Regulation, or when going beyond the letter of the law. These roles are but two sides of the same coin, since the "risks to data subject's fundamental rights and freedoms" are ultimately the cornerstone of both GDPRIAs and FRIAs as detailed in Figures 3 and 4.

That conception of the relationship between "risks" and "rights" under the GDPR echoes the "risk to a right" narrative proposed by Niels van Dijk et al. based on their interpretation of the ECtHR case law dealing with these notions.[110] The authors' analysis of the various risk-right logics in environmental, judicial and labour law led them to a conclusion that is similar to the one proposed in Section 2.3, which, is critical in properly understanding *what* DPIAs under Article 35 GDPR–as well as GDPRIAs and FRIAs, assuming that the "processing of personal data" is the "risk source" or the "event"–should aim to assess and mitigate. Putting the "data subject" in "data subject's rights and freedoms" is a *sine qua non* for DPIAs to fulfil their intended purpose and, *a fortiori*, for controllers to meaningfully realise data protection by design. While Section 2.3 came to a similar conclusion based on a formalistic assessment of the objective of the Regulation, the approach proposed by van Dijk et al. has the merit of being grounded in a solid jurisprudential analysis.

Building on the above interpretation, a thorough FRIA would require controllers to inventorise all their processing operations, pair each of them with the specific risks they raise for data subject's fundamental rights and freedoms, and deploy one or more controls to reduce their likelihood and/or severity to an appropriate level depending on the nature of the risk itself, as well as on all the other factors discussed above (Figure 8). How the "fundamental right" approach slots into the traditional risk management narrative is by influencing the types of risks that controllers must consider in their risk identification exercise. The same

109 See decisions 21/02293-10 (points 4.4 and 6.3, d), 20/02375-9 (pp. 3, 9), 20/02172-4 (p. 4) and 20/01896-3 (p. 5). The Irish DPC has voiced similar concerns in IN 19-7-2 (para 6.9).

110 More specifically, the second conception of the relation between rights and risks in the ECtHR case law on the intersection of environmental and privacy law discussed in point 2.3, para 3. See Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286, 294 <http://linkinghub.elsevier.com/retrieve/pii/S026736491500182X> accessed 18 march 2024.

can be said for GDPRIAs if considering the risk of non-compliance as the "risk source" and/or "event", and the operationalisation of the provisions contained in the Regulation as the "controls".

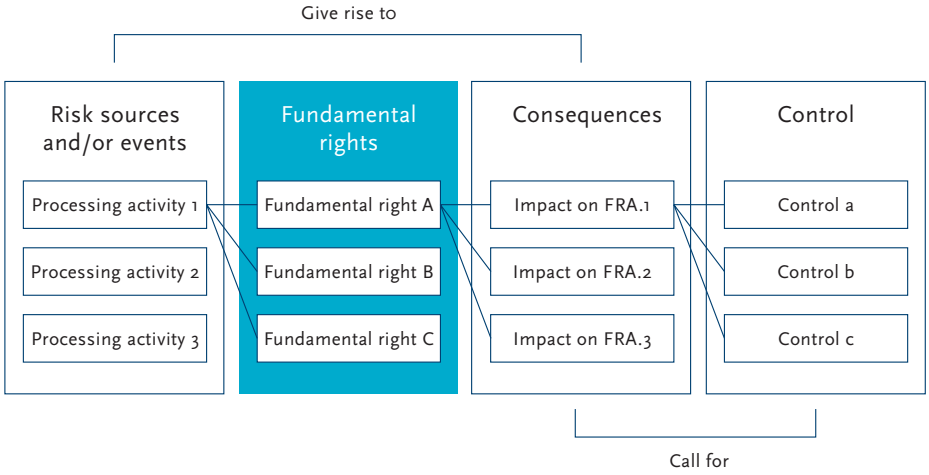

Figure 8. Components of a FRIA

3.4.2 The relationship between "processing" and "risks"

The risks that controllers must take into account and mitigate, states Article 25(1) GDPR, are those "*posed* by the processing" of one's personal data (emphasis added). Or, quoting Recital 75, those that "result from" such processing. How one interprets the causal relationship between the "processing" and the "risk" inevitably influences the material scope of data protection by design, and therefore the extent of the controller's risk management exercise. There are at least two ways to understand the wording used in the Regulation. Either one considers that, for a specific risk to fall within the remit of Articles 24(1) and 25(1) GDPR, the processing of personal data must be the *sole* causal factor. Or, one argues that it is sufficient that the processing of personal data *influences* the characteristics of the risk, either in terms of likelihood or severity, for it to fall within the material scope of Articles 24(1) and 25(1) GDPR and require the controller to implement appropriate technical and organisational countermeasures. Two elements seem to plead in favour of the second, broader interpretation. The first is teleological, and relates to the very objective of data protection by design. A restrictive interpretation of causality would indeed strip that principle from all substance by allowing controllers to bail on their obligations simply by invoking the existence of multiple causal factors. Since most risks, especially when it comes to the development and use of new technologies, result from the combination of different causes, that reading would render data protection by design virtually pointless. The second is semantic, and ties back to the use of "posed" instead of a more loaded term such as "caused", which would have inherited a long tradition of tort law interpretations.

The risk of addiction to social media makes for a prime example to illustrate the above. Social media platforms are indeed built to maximise user engagement, using UX tricks such as infinite scrolling and pop-up notifications. As such, their very design *already* raises addiction concerns.[111] Still, the processing of users' personal data to tailor their news feed *exacerbates* that risk by reinforcing the likelihood of that addiction actually developing, as well as its impact on the affected data subjects' mental health. The same can be said when it comes to personalised pricing, which can discriminate based on the currency used to pay for a certain good online, but is all the more effective when leveraging information such as

111 This short blog post summarises the main psychological mechanisms at stake: Kelsey Hansen, 'Our Social Media Addiction' [2022] *Harvard Business Review* <https://hbr.org/2022/11/our-social-media-addiction> accessed 27 March 2024; See also: Sandra Miranda and others, 'Addiction to Social Networking Sites: Motivations, Flow, and Sense of Belonging at the Root of Addiction' (2023) 188 Technological Forecasting and Social Change 122280 <https://www.sciencedirect.com/science/article/pii/S0040162522008010> accessed 27 March 2024; Yuxin Yang, 'Understanding Young Adults' TikTok Usage. Real People, Creative Videos That Makes Your Day' (UC San Diego 2020) <https://communication.ucsd.edu/_files/undergrad/yang-yuxin-understanding-young-adults-tiktok-usage.pdf> accessed 27 March 2024.

the buyer's previous transactions and purchase patterns. The fact that these risks, namely addiction and discrimination, would have existed *regardless* of any form of personal data processing is irrelevant if their *actual* manifestation, expressed in terms of likelihood and severity, partially result from the processing of users' personal data. In both cases, the respective controller will have to include these risks as part of their risk management exercise pursuant to Articles 24(1) and 25(1) GDPR (see Figure 9).

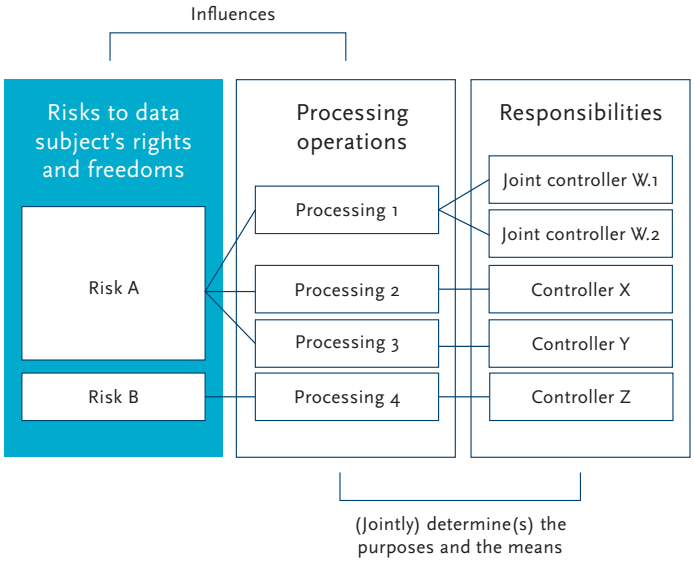

Figure 9. Causal relationship between the "risks" and the "processing"

3.4.3 Examples of "risks to data subject's rights and freedoms"

Now that the above paragraphs have clarified the concept and role of the "risks to data subject's rights and freedoms", comes the question of what these "risks" actually cover. While eliciting all the risks raised by the processing of one's personal data would be unrealistic, multiple sources provide more insights on what controllers are expected to mitigate. Recital 75 GDPR, for instance, mentions "the risk of physical, material or non-material damage", and lists the circumstances in which such damage would be particularly pronounced. While not explicitly referring to the *actual* risks posed for data subject's rights and freedoms, the list of "high risk" processing proposed in Article 35(3) GDPR and the nine criteria put forward by the WP29 in its Guidelines on DPIA provide a solid starting point for controllers to identify the type of activities that call for the implementation of stricter countermeasures.[112] Same goes for the list of "high risk" processing adopted by NSAs pursuant to Article 35(4) GDPR.[113]

NSAs have also flagged the risks raised by certain types of processing. Again, the goal of the present Section is not to come up with a comprehensive repository. Column K ("The risks of varying likelihood and severity for the rights and freedoms of natural persons") of the "Component of DPbD" Excel sheet is the closest attempt at such a catalogue, to which I redirect the reader. Some are nonetheless worth discussing here.

In decision IN 21-4-2, the Irish DPC highlighted that the way Meta Platform Ireland Limited had configured its Facebook Contact Importer, Messenger Contact Importer, Instagram Contact Importer and Messenger Search services, which allowed scrapers to retrieve the names and Facebook User IDs associated with specific telephone numbers, could lead to "identity theft, which could include using personal data to gain access to an existing account, or to contact friends and family of the data subject on the basis of their

112 See Section III, B, a) of Article 29 Working Party, 'Guidelines on DPIA' (n 97) 8–11.

113 The lists of "high risk" processing adopted by national supervisory authorities are available on the EDPB website <https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en?f%5B0%5D=register_decisions_topic%3A138> accessed 27 March 2024.

identity to defraud them" (para 73). It also noted that "merely knowing someone else's phone number can open them to sustained harassment from a former partner and indeed can heighten the risk of physical harm", and lead to other forms of "intimidation or coercion" (para 75). Such processing also made data subjects vulnerable to "robocall and smishing campaigns" (paras 76-77), as well as to "extensive fraud and impersonation such as SIM-swapping" (para 98). In decision IN-21-9-1, it also shortlisted the risks inherent to TikTok's public-by-default processing of "Child Users"'–that is, users *between 13 and 17*–social media content, including that of "losing autonomy and control over their data and, in turn, becoming targets for bad actors". This "could also lead to a wide range of potentially deleterious activities, including online exploitation or grooming, or further physical, material or non-material damage where [a child] inherently or advertently reveals identifying personal data". These come on top of the risks of "social anxiety, self-esteem issues, bullying or peer pressure" (para 91).

In a series of fines issued against Italian telecom operators, the Garante has underlined that the lack of proper control in the chain of acquisition of telephone numbers for telemarketing purposes, even when attributable to unofficial third parties, raises the risk of "nuisance calls" and paves the way for "identity theft, spamming and phishing activities".[114] In the same vein, the Polish regulator noted in decision ZSPR.421.2.2019 that unauthorised access by a third party to a customer database could lead to "spearphishing", targeted phishing boosted by social engineering techniques (p. 12).[115] Deficient security practices can also result in blackmail and intentional data leakage on the darknet, which might cause "long-lasting or even permanent damage", as noted by the Tietosuojavaltuutetun in decision 1150/161/2021 (p. 31). In the Mercadona case introduced in Section 2.3.2, the AEPD listed the many risks inherent to the roll-out of a surveillance system relying on facial recognition technology to ban individuals who have previously committed crimes from entering supermarkets, including the "risk of social exclusion and discrimination" (pp. 96-97), the "risk of long-term discrimination against persons with a criminal conviction, even after they have served their sentence" (p. 97), and the "risk of loss of freedom and privacy as no one behaves the same if they are being recorded or believe they are" (p. 99). In that, it is joined by the UODO that pointed, in decision DKN.5101.25.2020, the risks of "insurmountable disadvantages such as discrimination, social ostracism, feelings of stigma, stress or potential material losses" in a case in which the controller failed to securely store a list of persons undergoing quarantine due to a COVID-19 infection (pp. 9, 14).

3.4.4 Assessing and ranking the "risks"

A "risk" is typically expressed in terms of "likelihood" and "severity". Assessing that "risk" therefore involves quantifying *how likely* a certain scenario is to happen, as well as *how impactful* its materialisation would be for data subjects. Recital 76 GDPR laconically calls on controllers to evaluate the risks raised by their processing operations "on the basis of an *objective* assessment" (emphasis added). Yet, few metrics exist to quantify those properties, despite the pivotal role of such evaluation in both prioritising and tailoring the type of countermeasures that controllers must implement.

One could rank the "risks to data subject's rights and freedoms" according to the amount awarded in compensation by judicial authorities in the context of a claim based on Article 82(1) GDPR, since the notion of "damage" is but the consequence of the materialisation of a certain risk that can be expressed in terms of severity. In short, the higher the compensation, the more important the corresponding risk. Annika Selzer and her co-authors have explicitly vouched for that approach.[116] Bart van der Sloot's seminal work on "privacy harms" does not go as far as claiming that the amount of the monetary compensation should influence the seriousness of the underlying risk for the purpose of substantiating the risk-based approach.[117] Rightfully so, in my opinion, since the relevance of that metric presupposes that judicial case law exists on each type of risk. Yet, it is unlikely that all the risks raised by all possible types of processing activities have already materialised themselves in the first place. Even if that was the case, it would be improbable that

114 See, more specifically, decisions 9570997 (p. 24), 9485681 (p. 20) and 9435753 (p. 23).

115 The Wojewódzki Sąd Administracyjny upheld that decision on appeal in II SA/Wa 2559/19.

116 See, more specifically, point IV, 1. of: Selzer, Woods and Böhme (n 82) 460.

117 Bart van der Sloot, 'Where Is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights' (2017) 8 JIPITEC <http://www.jipitec.eu/issues/jipitec-8-4-2017/4641> accessed 28 March 2024.

data subjects have already claimed compensation for each type of material or non-material damage they might have suffered. For that metric to be meaningful, the amount of the compensation would also need to reflect the significance of the risk for data subject's fundamental rights and freedoms. This, however, would not be the case if a *serious* infringement only results in a *minor* inconvenience for the data subject. In other words, there might be a considerable disconnect between the risks raised by a certain processing operation on data subject's fundamental rights and freedoms–that should serve as the benchmark for controllers' risk management exercise pursuant to Articles 24(1) and 25(1)–and the concrete impact of that processing on a *specific* data subject–that should orient the competent judicial authority when calculating the amount of the compensation pursuant to Article 82(1) GDPR.

Another tempting ranking method would be to look at the fines issued by NSAs for various breaches of the Regulation, and posit that the higher the amount, the more important the principle the breach of which is sanctioned, and the more worthy of protection the corresponding fundamental right.[118] However, that approach suffers from much of the same shortcomings as the ones discussed above, in that it is also based on a *post-factum* assessment of a given scenario, rather than on an *anticipatory* evaluation of the risks raised by the processing at stake. Besides, the "nature of the infringement" is but one of the many elements that supervisory authorities must take into account when determining whether to impose an administrative fine and its amount. The weight of that criterion is therefore diluted in the calculation process, so that a high fine might be indicative of an infringement of a particularly important provision of the Regulation, but might also denote the controller's higher "annual turnover". Or an infringement of a higher "gravity" or of longer "duration". In that sense, any attempt at sorting the "risks" according to importance of the fine issued for an infringement of the corresponding provision of the Regulation will stumble against a "weighting" problem.

Scholars and practitioners have proposed methodologies to quantify the likelihood and severity of a given processing operation that move away from the conception of "risks" as threats to *organisations*, to instead consider the "risks" to *individuals*. Some are worth flagging here. Laurens Sion and his co-authors have presented a "data subject-aware" privacy risk assessment model to support privacy-focused threat modelling activities.[119] They introduced the concept of "Loss Magnitude" to capture the impact of the processing on data subjects by encompassing factors such as (i) the "Data Type Sensitivity", (ii) the "Number of Records", (iii) the "Data Subject Type" and (iv) the "Number of Data Subjects". Jason Cronk and Stuart Shapiro have proposed FAIR-P, a privacy-focused quantitative risk assessment methodology based on FAIR (Factor Analysis of Information Risk) that departs from security- and business-focused approaches by quantifying the "severity" of a specific processing with regard to its impact on "individuals".[120] NIST has developed its Privacy Risk Assessment Methodology, which considers "privacy events" as "potential problems *individuals* could experience arising from system, product, or service operations with data" (emphasis added).[121] Lastly, the CNIL has recently come up with knowledge bases as part of its PIA methodology in which it ranks the "severity" of a "risk" according to its impact on data subjects.[122]

118 See, more specifically, point IV, 2. of: Selzer, Woods and Böhme (n 82) 460.

119 Laurens Sion and others, 'Privacy Risk Assessment for Data Subject-Aware Threat Modeling', 2019 IEEE Security and Privacy Workshops (SPW) (IEEE 2019) <https://ieeexplore.ieee.org/document/8844608> accessed 4 April 2024; The authors had previously proposed to blend threat modeling and risk analysis in: Laurens Sion and others, 'Risk-Based Design Security Analysis' in SEAD '18: Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment (Association for Computing Machinery 2018) <https://doi.org/10.1145/3194707.3194710> accessed 4 April 2024.

120 As put by the authors, "rather than talking in terms of trade-offs in dehumanizing dollar figures, tangible impacts should be expressed in appropriate terms (such as deaths, suicides, imprisonments, embarrassments, etc.)". See: Jason Cronk and Stuart Shapiro, 'Quantitative Privacy Risk Analysis', 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (IEEE 2021) 342 <https://ieeexplore.ieee.org/document/9583709> accessed 4 April 2024.

121 National Institute of Standards and Technology, 'NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0' (NIST, 16 January 2020) <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf> accessed 4 April 2024.

122 Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) 3: Knowledge Bases' (n 14) 4–5.

4. Throughout the entire data processing life-cycle

While the previous sections relate to *what* controllers are expected to do, this one deals with the *when*. Article 25(1) GDPR indeed requires controllers to substantiate that risk-based approach "both at the time of the determination of the means for processing and at the time of the processing itself". The broad material scope of Article 25(1) advocated for in Section 2.3 elevates that timing dimension as a transversal modality of the risk management exercise that controllers must conduct to comply with that obligation.

4.1 At the time of the determination of the means

According to the EDPB, "the 'means for processing' range from the general to the detailed design elements of the processing, including the architecture, procedures, protocols, layout and appearance". Conversely, "the 'time of determination of the means for processing' refers to the period of time when the controller is deciding how the processing will be conducted, the manner in which the processing will occur, and the mechanisms which will be used to conduct such processing".[123] Therefore, and as clarified by the Belgian supervisory authority in decision 74/2020, "no actual processing needs to take place for data protection by design to be applicable". When it comes to cameras installed on a private property but partially overlooking a public area, argued the APD, "it is the specific nature of the installation of surveillance cameras and the taking of images with these cameras that require the implementation of technical and organisational measures". As such, "there *will* be at least one controller responsible for the installation of [these] cameras and the implementation of data protection by design, *regardless* of whether the installation of these cameras entails the processing of personal data" (emphasis added, paras 133 and 134).[124]

By decoupling the existence of a processing from the obligation to comply with Article 25(1), the Belgian authority raises an interesting conundrum. Data protection by design indeed only applies to "controllers", defined by Article 4(7) GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means *of the processing* of personal data" (emphasis added). Yet, since the chain of "processing" starts with the "collection" of the personal data at stake (Article 4(2) GDPR), an entity that determines the means of a processing that is *yet to happen* does not qualify as a "controller", and therefore falls outside the scope of Article 25(1). As soon as the envisaged processing debuts, though, that obligation will retroactively apply and hold that entity responsible for the choices made *at the time of the determination of the means* for that processing, *regardless* of whether it qualified as a "controller" back then. That scenario, however twisted, concerns all the actors that design their processing *before* even *collecting* any personal data.

The reference to the "means" for processing inevitably recalls the wording used in Article 4(7) GDPR to define the controller. This calls for two comments. First, the Board's interpretation of the "means" within the meaning of Article 25(1) GDPR aligns with that of its counterpart in Article 4(7). In both cases, states the EDPB, "determining the means" of a certain processing amounts to deciding "how" that processing is to be carried out.[125] Second, the syntactic similarities between both provisions suggest that the omission of the "purposes" from the wording of Article 25(1) GDPR is not accidental, but rather a deliberate choice of the EU legislator. The preparatory works confirm that intuition. The Parliament's position at first reading indeed proposed to extend the temporal scope of Article 23(1)–now 25(1)–to the "time of the determination of the *purposes* and means for processing". It also complemented that provision with an extra sentence that required data protection by design to "have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data". However, these amendments did not make it to the final text.

123 European Data Protection Board, 'Guidelines 4/2019' (n 12) paras 34 and 35, respectively.
124 For a similar reasoning in a comparable setting, see: NAIH/2020/2204/8 (p. 10).
125 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 35; European Data Protection Board, 'Guidelines 07/2020' (n 107) paras 33–35.

The decision to exclude the "time of the determination of the purposes for processing" from the temporal scope of Article 25(1) GDPR is questionable. First, it suggests that the "appropriate measures" that controllers must implement only make sense once they start discussing the *actual* implementation of their processing operations. However, as discussed and illustrated in Section 2, the notion of "measures" within the meaning of Articles 24(1) and 25(1) GDPR largely exceeds *technical* countermeasures, but also encompasses *legal* considerations as basic as the choice of the applicable lawful ground. Second, it is also at odds with the very objective of data protection by design, which is to ensure that controllers identify and mitigate the risks raised by their processing activities *as early as possible* to avoid having to make challenging and costly changes to a system that has already been designed. Yet, decisions concerning the "purposes" of the processing can drastically influence the type of risks posed for a data subject's fundamental rights and freedoms. In that sense, the temporal trigger of Article 25(1) GDPR does not always coincide with the moment at which the decisions shaping some of the most pressing risks are taken.

Yet, the practical impact of the absence of the "purposes" from Article 25(1) GDPR is rather limited. For one, the *material* scope of data protection by design remains unchanged. Indeed, the fact that the obligation kicks in later in the thought-process does not alter the substance of the risk management exercise. In that sense, controllers are still required to identify and mitigate *all* the risks posed by their processing operations *regardless* of the moment at which these risks were created. Second, the Board's interpretation of what constitutes the "essential means" of the processing is broad enough to encompass decisions that "are closely linked to the purposes and scope of the processing, such as the type of personal data which are processed, the duration of the processing, the categories of recipients, and of data subjects". Arguably, such a broad understanding of the "means" could push data protection by design earlier in the development process.

4.2 At the time of the processing itself

Not only must controllers consider appropriate measures "at the time of the determination of the means for processing", but they must also do so "at the time of the processing itself". As a result, notes the Board, controllers have "a continued obligation to maintain [data protection by design]", and "must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards".[126] Article 24(1) GDPR hints at a similar idea when stating that these measures "shall be reviewed and updated where necessary". The Polish UODO noted the importance of maintaining a high level of protection despite changes in the system in decision DKN.5130.2215.2020, highlighting that the "regular testing of the technical and organisational measures meant to ensure the security of the personal data processed, including the procedures used, also serves to ensure the fulfilment of the controller's obligation under Article 25(1) of Regulation 2016/679, i.e., to ensure that personal data protection is taken into account during the design phase, which also applies to *any changes made to the IT systems* used to process personal data" (emphasis added, p. 18). In that sense, complying with data protection by design is not a one-shot endeavour, but a dynamic exercise that spans the entire personal data processing lifecycle.

Speaking of "lifecycle", while Article 25(1) GDPR specifically targets the design (i.e. "the determination of the means") and operational (i.e., "the processing itself") phases, "there are no reasons to believe that the legislator did not want to refer to the whole lifecycle of a project", notes the EDPS. In short, controllers cannot simply identify and mitigate the risks raised by their processing operations at time T, but must continuously monitor the evolution of the different components of the risk-based approach listed in Articles 24(1) and 25(1) GDPR, and adjust their countermeasures accordingly. That includes taking stock of new entries in the state of the art, replacing outdated mitigations with objectively better ones, or rolling-out additional measures to supplement existing solutions. Likewise, the cost of implementation of a certain measure might have decreased since it was last considered by the controller, therefore making it a suitable option to address a particular issue at time T + 1. The controller could also have seen a surge in profits since the previous iteration of its DPIA that would justify the implementation of more expensive measure that

126 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 37, noting that "[o]nce the processing has started the controller has a continued obligation to maintain DPbDD, i.e., the continued effective implementation of the principles in order to protect the rights, staying up to date on the state of the art, reassessing the level of risk, etc".

only marginally improves the protection afforded to data subjects.[127] Similarly, the nature, scope, context and purpose of the processing might have changed since its inception, therefore affecting the types of risks it raises for data subject's fundamental rights and freedoms, or their likelihood and severity.

The obligation to continuously re-evaluate the appropriateness of these measures, highlights the Board, "also applies to pre-existing systems". As such, "legacy systems designed before the GDPR entered into force are required to undergo reviews and maintenance to ensure the implementation of measures and safeguards that implement the principles and rights of data subjects in an effective manner".[128] The mention of the "processing itself", in that sense, also prevents that processing activities the means of which have been determined prior to 25 May 2018 fall outside the scope of Article 25(1) GDPR–at least for the rare cases where such processing would not have undergone *any* change since the Regulation became applicable. Data protection by *re*-design might, however, prove tricky for businesses relying on a large volume of legacy software when compared to an actor developing a personal data processing system from scratch.[129]

One can conclude that the moment of the "determination of the means" does not always correspond to the earliest stages of software design, as the wording used by the Board seems to suggest.[130] As noted in Section 4.1, decisions as to the "how's" intervene throughout the entire lifespan of the supporting system. Since that first temporal criterion suffices to turn data protection by design into a continuous obligation, the added value of the "time of the processing itself", I argue, lies elsewhere. That is, in broadening the types of countermeasures that controllers must deploy, which should include data protection-conscious *design* choices (e.g., opting for federated machine learning instead of centralising the training datasets, or reducing the amount of recipients by cutting on processors), but also *runtime* mitigation strategies to ensure that the actual processing operations comply with the requirements stemming from the GDPR (e.g., logging each consultation of a database containing personal data, or verifying that the purpose of each further processing is compatible with one of the purposes specified for the collection) (see Figure 10). As a result, *every* decision that influences the way in which personal data are or will be processed either triggers the obligation to conduct the risk management exercise described in Figures 2 and 3, or to carry out a revision thereof.

127 Keeping in mind the dangers of relying on the resources available to the controller as a limiting factor in selecting the "appropriate" technical and organisational measures. See, on that point, Section 3.2.2.

128 European Data Protection Board, 'Guidelines 4/2019' (n 12) para 38.

129 As already noted by David Krebs, '"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, para 75 <https://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013-2-krebs.pdf> accessed 6 April 2024; 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) 101 <https://link.springer.com/chapter/10.1007/978-3-642-54069-1_6> accessed 6 April 2024; In the context of the 33rd International Conference of Data Protection and Privacy Commissioners held in 2011, the Information and Privacy Commissioner of Ontario even organised a dedicated parallel event on the issue entitled "Privacy by ReDesign: A Transformative Process". The full agenda is available on the conference website: <https://www.privacyconference2011.org/> accessed 6 April 2024.

130 More specifically, this follows from the future tense used in European Data Protection Board, 'Guidelines 4/2019' (n 12) para 35: "The 'time of determination of the means for processing' refers to the period of time when the controller is deciding how the processing *will* be conducted and the manner in which the processing *will* occur and the mechanisms which *will* be used to conduct such processing" (emphasis added).

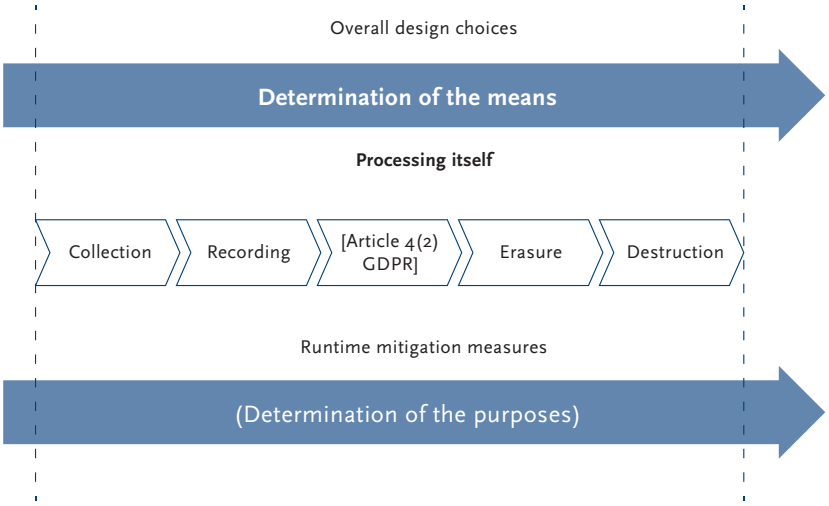

Figure 10. Temporal scope of data protection by design

4.3 The challenges of temporality à la Article 25(1)

As concluded above, data protection by design requires controllers to *continuously* assess and mitigate the risks raised by their processing operations for data subject's fundamental rights and freedoms, and update their countermeasures *every time* there is a change in the underlying system or in the chain of processing. Doing so in the current software production and implementation dynamic is no small feat, however. While the wording used the Regulation assumes a clear distinction between the moment of the "determination of the means for processing" and that of "the processing itself" (Article 25(1) GDPR), as well as a certain linearity in the processing chain that starts with the "collection" of personal data and ends with their "destruction" (Article 4(2) GDPR),[131] the reality of software development diverges from that simplistic representation. For two reasons, mainly.

4.3.1 Agile software development

First, the production of digital functionality has largely moved from linear approaches such as the "waterfall" development lifecycle model to "agile" methods. Under the former, software is developed in different stages–traditionally comprised of "requirement elicitation", "analysis", "design", "development", "validation", "deployment" followed by an "evaluation" period–, each of which must be completed before moving on to the next one.[132] Developing software using a waterfall model requires a clear vision of what the final product should look like right from the start of the project, precise planning and management, as well as extensive documentation.[133] Doing so takes time, lacks the flexibility to adapt to fast-evolving markets and needs, and runs the risk of postponing necessary quality and security changes to the end of the first iteration of the development lifecycle. To overcome these shortcomings, a group of developers compiled their vision of a more lightweight approach to software development in a "Manifesto for Agile Software Development",[134] in which they outlined the following *credo* (emphasis in original):

131 Michael Birnhack, Eran Toch and Irit Hadar, 'Privacy Mindset, Technological Mindset' (2014) 55 Jurimetrics 55, 35–37 <https://www.jstor.org/stable/24395620> accessed 6 April 2024. The authors observe that "[t]he law [Article 2(b) of Directive 95/46, NDLR] assumes a linear lifecycle" when it comes to the processing of personal data, starting with their "collection" and ending with their "destruction". However, they conclude, while "[t]he linear data collection and processing mindset and its segmentation fit many technologies with which we are familiar today and the business models that utilize these technologies", big data "defy many of these socio-technological assumptions".

132 Nayan B Ruparelia, 'Software Development Lifecycle Models' (2010) 35 ACM SIGSOFT Software Engineering Notes 8, 1–2 <https://dl.acm.org/doi/10.1145/1764810.1764814> accessed 6 April 2024. That waterfall approach, notes the author, has progressively been enhanced to include feedback loop so that each preceding stage could be revisited.

133 Christian Estler and others, 'Agile vs. Structured Distributed Software Development: A Case Study', *2012 IEEE Seventh International Conference on Global Software Engineering* (2012) 1199 <https://ieeexplore.ieee.org/document/6337393> accessed 2 April 2024.

134 Kent Beck and others, 'Manifesto for Agile Software Development' (2001) <https://agilemanifesto.org/> accessed 2 April 2024.

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

In short, the Manifesto values shorter development phases, continuous testing and regular communication with customers to ensure the "agility" and responsiveness of the process. As put by Seda Gürses and Joris van Hoboken, "agile programming practices allow developers across services to continuously tweak, remove, or add new features using 'build-measure-learn feedback loops'". In that sense, note the authors, "[w]eekly sprints, scrums and daily standup meetings are the rituals of this accelerated production", which includes "experimental features, minimum viable products and alpha releases, and may be best captured by the term 'perpetual beta' which stands for a never-ending development phase".[135] Agile methods are therefore particularly adequate when it comes to delivering value as early as possible with a baseline product that is meant to serve as the groundwork for further refinement in later iterations of the development project.

Besides, as software slowly moved from "shrink-wrap" products to "service-oriented architectures",[136] their respective risk profile became ever more dynamic.[137] It is indeed increasingly common for modern software to involve a prolonged relationship with end-users by offering a constant flow of new functionalities. The entanglement of production and use in a constant loop exacerbates the "evolving" nature of the risk these systems pose for individuals. As a result, note Gürses and van Hoboken, "'the beginning' of digital functionality that is offered as a bundle of services is hard to establish and, even if it could be established, not the only moment at which privacy by design is required".[138] Rapid changes might introduce new vulnerabilities. Assuming that the system involves the processing of personal data, such modifications are likely to raise additional risks for the data subject's fundamental rights, or affect the likelihood and severity of existing threats. This makes complying with data protection by design particularly complex, as controllers have to iterate over the risk management exercise described in Figures 2 and 3 with each new cycle.

In that sense, agile methods are both a bane and a boon–at least when it comes to complying with privacy and data protection law. On the one hand, shorter development phases mean more revisions, more risks to identify and mitigate, and, ultimately a heavier burden of compliance. On the other, a development rhythm involving frequent but incremental changes allows developers to surgically address the risks posed by the latest iteration of the software at stake *as they appear*, rather than postponing that exercise *at the end of the first full cycle*, when it might be challenging to revert certain technical decisions. Doing so, however, requires the implication of a tech-savvy legal during each successive "spike" in the development process, and posits that controllers have the financial and intellectual resources to spare. In short, agile methods are not only *compatible* with the very idea of data protection by design, but also a formidable *opportunity* to unlock its full potential, *provided that* controllers are adequately equipped to support that sort of interdisciplinary endeavour. One could draw inspiration from the "methodology proposed by the French Agence Nationale de la Sécurité des Systèmes d'Information ("ANSSI") to integrate security considerations throughout a typical agile development lifecycle,[139] and adapt it to fit the requirements of the GDPR.

135 Seda Gürses and Joris van Hoboken, 'Privacy after the Agile Turn' in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018) 593 <https://www.cambridge.org/core/books/cambridge-handbook-of-consumer-privacy/privacy-after-the-agile-turn/95580B93B4B2446DC5B59166FD2A732F> accessed 27 March 2024. As such, "[m]inor changes to existing features happen daily, while major changes can be introduced every two weeks to two months".

136 Gürses and van Hoboken (n 135) 583–584.

137 On that note, it is also worth noting that the dynamic nature of software's risk profile has been one of the main drivers for the revision of the current EU regulatory framework on product liability. See, more specifically: Christiane Wendehorst and Yannic Duller, 'Safety and Liability Related Aspects of Software' (De Gruyter 2022) Report 26 <https://www.degruyter.com/document/doi/10.1515/9783110775402-002/html> accessed 22 March 2024.

138 Gürses and van Hoboken (n 135) 592.

139 Agence Nationale de la Sécurité des Systèmes d'Information and Directeur interministériel du numérique et du système d'information et de communication de l'État, 'Agilité & Sécurité Numériques - Méthodes et Outils à l'usage Des Équipes Projet' <https://cyber.gouv.fr/publications/agilite-et-securite-numeriques-methode-et-outils-lusage-des-equipes-projet> accessed 22 March 2024.

4.3.2 From "coding" to "assembling"

Second, software developers rarely start coding from scratch, but instead build on existing components such as Software Development Kits ("SDKs") and Application Programming Interfaces ("APIs"). These resources can be used as starting points to develop platform-specific applications and programmes, or integrate certain functionalities such as login, geolocation, payment or advertising services. While these third party tools drastically streamline the development process by circumventing the need to constantly "reinvent the wheel", they also pave the way for the introduction of security vulnerabilities,[140] and run the risk of triggering unexpected processing activities. Developers should therefore be particularly careful when integrating bits and parts of code written by third parties.

In cases where the integration of an SDK, an API or any other third party library results in the processing of personal data, the entity that decided to rely on that component is likely to be regarded, alone or together with the entity responsible for its development, as the one determining the "purposes" and the "essential means" of the said processing, thereby triggering the obligation to implement appropriate technical and organisational measures to ensure and demonstrate compliance with the Regulation. The *Fashion ID* decision is a case in point. Building on its jurisprudence in *Wirtschafstakademie* and *Tietosuojavaltuutetun*, the CJEU ruled that the operator of a website was to be considered as a controller, jointly with Facebook, for the "collection and disclosure by transmission of the personal data of visitors to its website" resulting from the implementation of Facebook's "Like" social plugin on its web pages.[141] Since the decision to integrate third party components amounts to determining parts of the "means" for processing, it also triggers the applicability of Article 25(1) GDPR, as detailed in Section 4.1.

The CNIL Developer's Guide lists some of the countermeasures that controllers might want to implement when relying on software components written by third parties.[142] These include carefully assessing their added value, activating only the strictly necessary features, selecting maintained libraries, APIs and SDKs, and securing a valid lawful ground for the processing triggered by the integration of that specific resource.[143] The French regulator also notes the importance of configuring off-the-shelf solutions to avoid security holes, auditing each component to map their own dependencies, and regularly updating these components, or phasing out libraries, APIs and SDKs that have reached the end of their support lifecycle. The Garante hammered on that point in decision 9790365, in which it fined a healthcare facility 70.000 euros for failing to tweak the default access control settings of an information management system developed by a third party so to limit access to patients' data to the personnel actually in charge of their treatment, instead of using a single authorisation profile shared by all its employees (pp. 5, 10).[144]

Since relying on third party components makes the controller vulnerable to any change imposed by the developers of these dependencies, monitoring their evolution and periodically reviewing their functioning is paramount in ensuring that the processing activities it is responsible for remain compliant with the Regulation over time. Doing so is all the more important when the developers of these building blocks do not qualify as either (joint) controllers or processors, but instead act as third parties within the meaning of Article 4(10) or mere "producers of products, services and applications" as understood in Recital 78, and therefore fall outside the personal scope of application of Article 25(1) GDPR. In that sense, relying on code written by third parties, or contributing to a supply chain composed of many different, yet interdependent

140 For an overview of the most common security risks raised by APIs, see the 2023 iteration of OWASP's Top 10 API Security Risks, which is accessible here: OWASP, 'Top 10 API Security Risks – 2023' (OWASP, 2023) <https://owasp.org/API-Security/editions/2023/en/0x11-t10/> accessed 22 March 2024.

141 *Fashion ID* (n 20) para 84.

142 Commission Nationale de l'Informatique et des Libertés, 'GDPR Developer's Guide' (n 14). See, more specifically, 'Sheet n°09: Control your libraries and SDKs' <https://www.cnil.fr/en/sheet-ndeg09-control-your-libraries-and-sdks> accessed 6 August 2024.

143 This is particularly important since, as noted by the Court in *Fashion ID* (n 20) 102, it is up to the party embedding a third party plugin, as joint controller, to obtain the valid consent of the data subjects for the collection and transmission of personal data triggered by the integration of that plugin.

144 The Garante deployed a similar reasoning in decisions 9768363 (p. 14), 9685994 (pp. 3-4, 14), 9685922 (p. 12) and 9675440 (pp. 3-5, 26). Along the same lines, see the Norwegian Datatilsynet's decision in 21/00480-10 (pp. 3, 6), which led to a 4.000.000 NOK fine for the Østre Toten municipality.

actors exposes *controllers* to potential infringements caused by entities that do *not* qualify as such with regard to the processing at stake, and therefore face limited responsibilities. This, in turn, is a source of misalignment between the allocation of responsibilities pursuant to the GDPR, and the *actual* influence over their design. The quintessential challenge of temporality à la Article 25(1) GDPR is therefore for controllers to develop processes and tools to integrate data protection considerations within their own software development lifecycle, while ensuring that the dependencies they rely on do not compromise their efforts.

5. Wrapping up, looking ahead

177 decisions later, is now time to reflect on the main lessons learned from the case law review (Section 5.1). The moment is also ripe to build on the knowledge amassed along the way to answer the research question that drove this contribution in the first place, i.e., what is the exact scope of controllers' obligations under Article 25(1) (Section 5.2). Lastly, one should assess whether that provision is, as often regretted in literature, indeed too vague to be enforced (Section 5.3).

5.1 Drawing the conclusions from the case law review

As already noted in the Introduction, I ought to point the reader to a similar initiative piloted by Christina Michelakaki and Sebastião Barros Vale from the Future of Privacy Forum ("FPF").[145] Some scoping and methodological differences aside, the FPF report nicely complements the findings outlined in this paper. First among these findings, is that NSAs never rely on Articles 24(1) or 25(1) GDPR as the *sole* basis for a sanction, be it a warning, a reprimand, an order to comply, a definitive or temporary ban, or a fine. The recent decision IN 21-4-2 issued by the Irish regulator against Meta 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 to substantiate the *purpose limitation* and *integrity and confidentiality* principles. The same can be said for the 345,000,000 EUR fined the DPC imposed on TikTok in decision IN-21-9-1, which sanctioned the failure to identify the risks posed by the public-by-default processing of children' social media content, and to appropriately comply with the principles of *fairness* (Article 5(1)a), *data minimisation* (Article 5(1)c), *integrity and confidentiality* (Article 5(1)f) as well as *data protection by default* (Article 25(2)). This is hardly surprising since, as discussed in Section 2.3, Articles 24(1) and 25(1) GDPR require controllers to mitigate *both* the risks of non-compliance with the provisions of the Regulation ("Risk assessment layer 2" in Figure 1) and the additional risks raised by the processing at stake for data subject's fundamental rights and freedoms ("Risk assessment layer 3" in Figure 3).

Second, NSAs regularly throw Articles 24(1) or 25(1) GDPR among the list of infringements in situations where a controller has failed to comply with one or more provisions of the Regulation *by design*, but *without specifying the exact reasons* that warrant their inclusion as a ground for sanction. Building on that narrative, and since infringing a given rule or principle *necessarily* implies that the controller has failed to proactively implement the technical and organisational measures that would have prevented non-compliance, regulators seem to frequently include data protection by design in their decision for the sake of it, rather than to sanction a violation of one of the components that make it a standalone obligation. The amount of "Nothing specific" entries in the "Components of DPbD" Excel sheet is symptomatic of that tendency to often routinely, almost mechanically, refer to Articles 24(1) or 25(1) despite the absence of any concrete argument about, say, the unappropriateness of the measure chosen by the controller, a deficient review of the state of the art, or the untimeliness of the risk assessment process. Doing so, I argue, risks dwindling the impact of Articles 24(1) and 25(1) by relegating these provisions to an ornamental role.

Third, NSAs often fail to provide the full assessment of the different elements listed in Articles 24(1) and 25(1) GDPR to support their finding of non-compliance with data protection by design. Instead, most decisions start with an exposé of the facts and applicable regulatory framework, followed by the position of the authority on whether the former constitutes an infringement of the latter. In short, while the *outcome* of

145 Michelakaki and Barros Vale (n 3). See, more specifically, their conclusions on 59-62.

the regulator's own risk assessment process is always apparent from the decision, the *criteria*, as well as the *role* they played in orienting its conclusion, are seldomly discussed. Looking at the cost of implementation, for instance, a quick look at the dedicated column in the "Component of DPbD" Excel sheet reveals that few decisions actually detail *how* that cost was calculated, let alone the *weight* attributed to that factor when deciding whether a controller was supposed to implement a particular countermeasure. What led the Irish DPC to conclude, in case IN 21-4-2, that stricter rate limiting and bot detection measures, captchas and red teaming initiatives "were all viable existing measures" for Meta Platform Ireland is, for instance, nowhere to be found. The same holds true for the other elements of the risk-based approach, an *overview* of which is generally provided in each decision, but the *impact* and *weight* of which is often missing from the reasoning.

Fourth, NSAs frequently limit their reasoning to whether a controller has or has not implemented appropriate technical and organisational measures. Only rarely do they supplement their analysis with concrete recommendations as to what the controller *could have* done differently. The main lesson one can draw from a decision is therefore generally limited to an *a contrario* reading of its outcome. This leaves controllers reasoning by analogy to try and guesstimate the best course of action in their particular situation. Not to mention that one supervisory authority's opinion on a given issue might differ from another's, a scenario that cannot be excluded for decisions that have not gone through the cooperation and consistency mechanism either because the decision does not concern a "cross-border processing" within the meaning of Article 4(23) GDPR, or because it was treated as a local case under Article 56(2). Of course, one might argue that issuing precise guidelines does not fall within the remit of administrative and judicial authorities when *enforcing* the Regulation. Still, clear indications as to what constitutes the "state of the art" in terms of "appropriate technical and organisational measures" is sorely lacking,[146] and once again calls into question the decision to ditch initiatives such as ENISA's online PETs repository.

5.2 Circling back to the research question

Building on the overall findings of the case law review, this paper shed light on the three core components of data protection by design. The following paragraphs highlight some of the key takeaways from that exercise. First, "measures" come in all sizes and shapes, even though NSAs have so far mostly sanctioned the lack of risk assessment process, documentation, policies, access control, encryption, testing and evaluation protocols, and awareness raising activities. Putting too much emphasis on their "technical" or "organisational" nature, I argued, would water down the level of protection afforded to data subjects. The combined reading of data protection by design with the overarching objective pursued by the GDPR as a piece of secondary law suggests that the measures controllers ought to implement pursuant to Article 25(1) are not limited to ensure compliance with the provisions that are *strictly* contained in the Regulation, but to protect *all* data subjects' fundamental rights and freedoms with regard to the processing of their personal data, including but not limited to privacy and data protection. In that sense, I concluded, data protection by design offers a tinted window on the Charter.

Second, the different elements controllers must take into account when selecting their countermeasures are truly what makes data protection by design an indispensable "purveyor of flexibility", a buffer zone of sorts that allows regulators to shape the way controllers are to substantiate the rigid principles and rules of the Regulation in concrete scenarios. Despite discontinued attempts in the past, the "state of the art", I noted, would benefit from a degree of community outsourcing. The "cost of implementation" should be understood as the net cost for controllers after factoring in the benefits such implementation entails in terms of avoided fines, damages, and reputational harm. While tempting, it should also not be confused with the controller's available resources, as it would allow controllers to hide behind the lack of sufficient resources to justify the absence of "appropriate" measures. NSAs, on their end, should ensure that the cost of non-compliance, which mainly–if not exclusively–takes the form of fines, always remains higher than the cost of compliance. The "nature, scope, context and purposes" of the processing is to be understood as,

146 Michelakaki and Barros Vale (n 159) 62, also close their own case law review by underlining that "[a] non-exhaustive list of technical measures that have the potential to secure alignment with DPbD&bD rules, as well as the role that different emerging PETs play in that context, may prove invaluable for controllers who invest in technology to safeguard data subjects' rights and freedoms".

respectively, its inner characteristics, the amount of data subjects concerned, the circumstances in which it is deployed, and the objective it pursues–keeping in mind that the GDPR itself provides for a specific regime regarding certain well-defined purposes. Lastly, the "risks for [the] rights and freedoms of natural persons" appears to play a double role, as it both covers *what* is to be mitigated, and influences *how* controllers must do so.

Third, the use of the "determination of the means" as the temporal trigger for the application of Article 25(1) is already enough, I argued, to turn data protection by design into a continuous obligation. The added value of extending that provision to the "time of the processing itself", I therefore posited, lies in broadening the types of countermeasures that controllers must deploy, which should include both data protection-conscious *design* choices, but also *runtime* mitigation strategies to ensure that the actual processing operations comply with the requirements of the GDPR. The progressive shift to agile software development is, in that sense, both a boon and a bane when it comes to complying with data protection by design, as shorter development cycles allow for incremental changes, *provided that* controllers can spare the human and financial resources to do so. Similarly, the use of dependencies such as SDKs and APIs developed by third parties that do *not* qualify as (joint) controllers with regard to a certain processing exposes the *actual* controller to a breach of data protection be design, even where the allocation of responsibilities and the concrete influence over the design of that dependency do not align.

5.3 Overcoming the "vagueness" of Article 25(1)

As discussed in Section 2.1, the open-ended nature of Article 25(1) has been a common ground for criticism. While there is no denying the vagueness of that provision, this is, I argue, is a feature rather than a bug. Providing clear guidance on how to substantiate Article 25(1) within the text of the Regulation itself would have defeated its purpose, i.e., compelling controllers to mitigate all the risks raised by their processing activities *regardless* of the evolution of technology. While this comes at the cost of upfront legal certainty, it is a necessary trade-off to guarantee that data protection by design remains relevant over time. That flexibility is the essence of the risk-based approach, and what makes the combined reading of Articles 5(2), 24(1), 25(1) and 35 the "keeper of relevance" of the GDPR. The reasoning deployed in case C-129/21 perfectly illustrates that point. The Court expressly relied on the "broad wording and scope of Articles 5(2) and 24(1)" to oblige Proximus to implement "appropriate technical and organisational measures" to notify a request for erasure not only to the *recipients* of the personal data as required by Article 19 GDPR, but also to "the telephone service operator *who has supplied it with such personal data* (emphasis added)".[147] In doing so, the CJEU leveraged "accountability" as a lens through interpreting *another* provision of the Regulation, thereby illustrating its role in keeping the GDPR effective.[148] The "Type(s) of measure(s)" column of the "Components of DPbD" Excel sheet is a testimony to the role of data protection by design as the Regulation's primary source of resilience in a fast-evolving digital landscape.

Rubinstein and Good feared that "imposing large fines on companies that violate Article 25 would [be] improper given the lack of clarity over what Article 25 requires or how it relates to other more substantive provisions".[149] Lee Bygrave augured–rightfully so–that "[i]nvoking stiff sanctions for a breach of Article 25(1) will not be easy given the very general (and process-oriented) way in which its obligations are formulated".[150] Yet, NSAs started to do it anyway. In fact, 353 out the 3089 administrative and judicial decisions indexed on GDPRhub on 31 December 2023 mention either Article 5(2), 24(1) or 25(1), or a combination thereof, accounting for more than 11% of the database. A quick look at the GDPR Enforcement Tracker confirms that trend, as 167 of the 2173 entries on the platform rely *specifically* on Article 25(1). Besides, some of the highest fines ever levied sanction a breach of data protection by design–if among other provisions–, including the 405,000,000 EUR, 265,000,000 EUR and 17,000,000 EUR fines issued against Meta in decisions

147 See *Proximus v Gegevensbeschermingsautoriteit*, Case C-129/21, Opinion of Advocate General Anthony Michael Collins [2022] electronic Reports of Cases (ECLI:EU:C:2022:332) para 67; *Proximus v Gegevensbeschermingsautoriteit* (n 86) para 83.

148 Such a reading, emphasised the Court, is necessary "to guarantee the effectiveness of the right to withdraw consent provided for in Article 7(3) of the GDPR and to ensure that the data subject's consent is strictly linked to the purpose for which it was given". See *Proximus* (n 86) para 85.

149 Rubinstein and Good (n 37) 55.

150 Bygrave (n 9) 117.

IN 20-7-4, IN 21-4-2 and IN 18-11-5, the 345,000,000 EUR fine issued against TikTok in decision IN-21-9-1, the 27,802,946 EUR fine issued against TIM in decision 9256486, and the 16,729,600 EUR fine issued against Wind Tre in decision 9435753.

This is not to say that NSAs always *meaningfully* enforce data protection by design. As hinted at in Section 5.1, regulators could detail the reasons for including Articles 24(1) and/or 25(1) in the list of infringements. Similarly, they could substantiate the thought-process behind the assessment of the different elements of the risk-based approach, especially when it comes to the criteria used, their exact role, as well as their weight in the decision-making process. This is particularly relevant for the analysis of the "state of the art" and the "cost of implementation", as clearer explanations on these aspects would provide controllers with actionable knowledge–and would be welcome for the other two components. These aspects are likely detailed in the conclusions exchanged by the parties involved in the proceeding, or in the report occasionally issued by the regulator's investigating body. But none of these documents are typically made public. Integrating parts of that reasoning–or a redacted version thereof–directly within the text of administrative decisions would go a long way towards fleshing out the contours of that provision, and nudge controllers on the right track.

The value of data protection by design, I would conclude, lies precisely in the enforcement ecosystem built around it, which is composed of national supervisory authorities acting in their enforcement and advisory capacity under both the Board's and Supervisor's umbrella. The findings detailed in this paper are, in that sense, also valuable to interpret other risk-based regulatory frameworks such as the AI Act.[151] Sure, deriving a comprehensive catalogue of "appropriate" measures from administrative jurisprudence is likely to take years. Granted, any attempt at doing so will have to cope with the incredibly fast pace at which technology evolves. But most decisions bring their share of clarifications, however pertinent, as to *how* controllers are expected to give effect to an obligation that was conceived to withstand the test of time and, therefore, must mature before reaching its full potential. Criticising Article 25(1) for its lack of *implementation* details would, in that sense, amount to disapproving its very *nature*. The ramping up of NSAs' enforcement efforts, soon to be smoothened by the upcoming Regulation harmonising certain procedural aspects of GDPR enforcement,[152] heralds, I like to think, promising days for data protection by design.

151 It is worth noting that the final text of the AI Act includes an obligation for law enforcement authorities using real-time remote biometric identification systems in publicly accessible spaces and users of high-risk AI systems to carry out a FRIA–if not within the same meaning of the FRIA understood in the context of the present paper–, and lists the minimum elements it should include. See: European Parliament, 'European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))' [2024] OJ C138/TA <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html> accessed 2 April 2024, arts 5(2) second indent, 27.

152 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Additional Procedural Rules Relating to the Enforcement of Regulation (EU) 2016/679' COM (2023) 348 final <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3A52023PC0348> accessed 2 April 2024.