MAY 2023

Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR

FUTURE OF PRIVACY FORUM

AUTHORED BY

Christina Michelakaki and **Sebastião Barros Vale**

EDITORS

Dr. Rob van Eijk
Dr. Gabriela Zanfir-Fortuna
Isabella Perera
for the Future of Privacy Forum

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

FPF Europe maintains strong partnerships across the EU through its convenings and knowledge-sharing with policymakers and regulators. This transatlantic engagement helps regulators, policymakers, and staff at European Union data protection authorities better understand the technologies at the forefront of data protection law. By building this bridge between European and U.S. data protection cultures, FPF hopes to build a common data protection language. Learn more about FPF Europe by visiting fpf.org/EU.

TABLE OF CONTENTS

BACKGROUND AND OVERVIEW

The European Union's (EU) General Data Protection Regulation (GDPR) introduced the concept of data protection by design and by default (DPbD&bD) in its Article 25.[1] This provision enshrines two key obligations that the controller should abide by, as it mandates: 1) the adoption of technical and organizational measures (TOMs) — both at the time of the determination of the means and during the processing, designed to implement data protection principles into the processing, generally meet the requirements of the GDPR and protect the rights of individuals whose personal data are processed, and 2) ensuring that, by default, only personal data necessary for each specific purpose are processed.

Given the breadth of the obligations, it has been argued that the "entire weight of the GDPR rests on the 'shoulders' of Article 25."[2] It is also noted that Article 25 is making the GDPR "stick" by overcoming "the gap between 'law in books' and 'law in practice.'"[3] The DPbD&bD obligation is seen as a tool to enhance accountability for data controllers, implement data protection effectively, and add emphasis to the proactive implementation of data protection safeguards.[4]

This Report aims to explore how the DPbD&bD obligation breaks down in practice and whether it is effective, informed by how Data Protection Authorities (DPAs) and Courts enforced Article 25 GDPR since it became applicable. For instance, we analyze whether DPAs and courts find breaches of Article 25 without links to other infringements of the regulation and what provisions enforcers tend to apply together with Article 25 the most, including the general data protection principles and requirements related to data security under Article 32. We are also looking at what controls and behavior of controllers are deemed to be sufficient to comply with Article 25 and, per a contrario, what is not sufficient.

This analysis is all the more important, with novel technologies involving very complex personal data processing, like Generative AI, being built and deployed on the market, raising data protection concerns.[5] Understanding how this obligation manifests in practice and what are the requirements of DPbD&bD may prove essential for the next technological age.

To compile the Report, we looked at publicly available judicial and administrative decisions and regulatory guidelines across EU/EEA jurisdictions and the UK, complemented by press releases and annual reports. The research is limited to documents released before March 2023 (listed in Annex I) and includes information from 92 cases — 10 court rulings and 82 enforcement decisions issued by national DPAs — and guidelines from 16 EEA Member States, the UK, and the European Data Protection Supervisor (EDPS).[6] The decisions mentioned in the Report are merely a fraction of all the decisions we found in our research; Article 25 GDPR was mentioned in more than 150 decisions issued by European DPAs that we were able to identify. In this Report, we decided to narrow down and dive deeper into the cases that we found to be the most important in terms of the data processing context, the underlying legal reasoning, and the consequences for the parties involved, as well as the application of Article 25 GDPR more generally in the EEA and UK.

Each case summary throughout the Report can be identified easily by a code that is a combination of the country's abbreviated name and a number (e.g., IE1, which refers to the first Irish DPA case discussed in this Report, will be referenced multiple times in different sections); summaries related to court rules include "CR" in their code (e.g., BE-CR-1, which refers to the first Belgian court ruling discussed in this Report). In Annex I of the Report, we compile the references to all the cases that we analyze throughout the Report. Annex II offers a comparative overview of the DPA decisions, with a focus on the number of decisions and the total monetary sum of administrative fines issued in each country in Euros (EUR).

The cases we identified involve different degrees of complexity of the processing of personal data at issue, from the mundane to cutting-edge technology, including:

- Accessing online services and platforms — from social media, to delivery services via mobile apps to gaming;
- Processing of personal data through an "emotion recognition" AI system for customer support;
- Live facial recognition to manage access on premise;
- Processing of health records in a hospital, for instance, management of personnel access rights to health records, or making available health results online in an environment prone to vulnerabilities;
- Delivery of parcels to customers' homes;
- Use of technological tools in an educational context, such as online proctoring and automated grading of students; and
- Processing of personal data in the context of employment, such as monitoring employee location data or the use of a whistleblowing application.

The comparative reading of relevant cases shows divergence in how DPAs interpret the preventive nature of Article 25 GDPR. While some of them are reluctant to find a violation of Article 25 if an incident constituted an isolated case or where no principle in Article 5 GDPR was violated yet, others apply Article 25 preventively before further GDPR breaches occurred or even before the planned data processing took place. The analysis of existing case-law indicates that Article 25 applies to not only information systems but also business and human processes, training, and other contexts relevant to personal data processing.

An important insight that surfaced during our research is that most DPAs show reluctance to formulate what would be an appropriate protective measure and also to explicitly outline the role of Privacy Enhancing Technologies (PETs). All of the sections of the Report are accompanied by summaries of cases and brief analysis pointing out commonalities and outliers. Identifying enforcement trends, particularly divergent ones, is essential to understand what areas need further clarification from the European Data Protection Board (EDPB) and the Court of Justice of the European Union (CJEU).

Ultimately this Report shows that Article 25 GDPR, despite its novelty in the data protection legal regime and despite criticism that it relies on vague and abstract wording, has been enforced in numerous cases in the first five years of the GDPR being applicable.

The Report starts by exploring the history, context, and limitations of Article 25 (Section 1). Section 2 then delves into the enforcement record of DPAs on Article 25 (Section 2). Section 3 discusses how Article 25 has been applied in sectoral areas, highlighting clusters of cases in direct marketing, privacy preservation in online environments and the role of PETs, and the use of technological tools in education contexts (EdTech). Finally, Section 4 will lay out some of the identified legal interpretation and application trends that surfaced during our research and highlight remaining areas of legal uncertainty that may be clarified in the future by regulators or the CJEU.

1. THE FUNDAMENTALS OF DATA PROTECTION BY DESIGN AND BY DEFAULT IN THE GDPR

Article 25

Data protection by design and by default

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

2. The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

1.1. Origins and status of Data Protection by Design and by Default, from broad policy goal to legal obligation under the GDPR

The concept of Privacy by Design was initially proposed by the Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian, in the 1990s.[7] Subsequently, it was acknowledged as a component of fundamental privacy protection in 2010 at the annual assembly of International Data Protection and Privacy Commissioners,[8] and it was recognized in 2012 by the US Federal Trade Commission (FTC) as a practice for protecting online privacy.[9] The GDPR has fully incorporated DPbD&bD by obligating controllers to implement appropriate TOMs both by design and by default in order to meet the requirements of the GDPR and protect data subjects' rights and freedoms.[10]

Article 25 GDPR is a novel provision under EU law; the 1995 Data Protection Directive (DPD), the precedent of the GDPR, did not specifically address the concept of DPbD&bD.[11] The Directive briefly touches on the idea in Recital 46, where it states that the controller needs to take TOMs by design with a limited scope, stating that these measures should merely aim "at maintaining the security and thereby to prevent any unauthorized processing." Similarly, the measures mentioned under Article 17 of the Directive focused solely on the security of the processing. The Council of Europe's Convention 108+ has a more directly relevant DPbD&bD provision without focusing on security.[12] Specifically, Article 10(2) notes that "each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing and shall design the data processing in such a manner as to prevent or minimize the risk of interference with those rights and fundamental freedoms."[13] The difference between the provisions of Convention 108+ and those of Article 25 of the GDPR lay on the absence of data protection by default requirements in the former, which is a requirement that is found in the latter.

DPbD&bD is included both in the GDPR and the Directive on Data Protection and Law Enforcement.[14]

The European Court of Human Rights (ECtHR) has arguably recognized DPbD&bD as a requirement under Article 8 of European Convention on Human Rights (ECHR),[15] and the EU Charter of Fundamental Rights (EUCFR) contains a "homogeneity clause" that ensures the protection of the Charter rights does not fall below the level of protection provided by the Convention rights.[16] Also, the CJEU has implied that Article 8 of the EUCFR, which deals with data protection, requires the adoption of TOMs to ensure effective protection of personal data.[17] It was argued in literature that "DPbD&D requirements may operate independently of Article 25 GDPR, and Article 20 LED" and "DPbD&D has to be regarded as a key principle in European data protection law and not as a mere rule given its 'level of abstraction, open-endedness, and persistence'".[18]

In 2023, the International Organization for Standardization (ISO) adopted Privacy by Design as a norm in ISO 31700, which lays down 30 requirements for embedding data protection into consumer products and services.[19] With regards to this development, it has been noted that "conformity with the ISO standard does not equate to complying with the GDPR (and vice versa), and businesses looking to adhere to the GDPR must still observe its requirements separately."[20] However, conformity with the ISO standard may be useful in proving compliance, building trust, and gaining a strategic advantage over competitors.

Finally, the discussion on the nature of Article 25 GDPR will come up as a recurrent theme in this Report. While certain DPAs are willing to take on board the preventive capabilities of DPbD&bD — admitting for instance, that a breach of Article 25 can take place in relation to setting up the

conditions for processing personal data even where the actual processing has not taken place, others are reluctant to say that Article 25 GDPR could constitute a basis for corrective action irrespective of the existence of actual processing.

1.2. Perceived limitations of Article 25 GDPR: vague wording, limited personal scope

It has been argued that the language of Article 25 GDPR is vague and complex, making it difficult to incentivize and achieve DPbD&bD.[21] This lack of clarity is also reflected in the flexibility given to controllers to decide on the appropriate measures, given that the GDPR does not include specific technical standards. On a similar note, it has been claimed that Article 25 "is poorly aligned with privacy engineering methods and practices," a subject which we explore in the ensuing section.[22] Others, however, have challenged these claims by noting that DPbD&bD require the implementation of "already existing obligations resulting from intrinsic features of personal data processing."[23]

In any case, lack of clarity can lead to inconsistent implementation among organizations and confusion in understanding the mandate of Article 25, in particular among smaller businesses. Similarly, organizations may face challenges and incur costs when retrofitting existing products and services to conform with the requirements of Article 25 GDPR.

Also, the reach of Article 25 GDPR is limited as it primarily applies to data controllers, but not all entities involved in the development and use of information systems and data processing operations fall under this category. This limitation deserves further attention. However, it is certain that before acting as processors, the same entities may act as controllers at the stage of developing a product or service that will subsequently process personal data on behalf of others. Additionally, the relationship between controllers and processors is under increased scrutiny when compliance with Article 25 GDPR is assessed, as it is clearly visible from the cases analyzed in Section 2.1.a below. For instance, failure to carry out audits, including inspections, of the processor was found to be a violation of Article 25(1) GDPR (see case PL1).

1.3. Privacy Enhancing Technologies (PETs) support DPbD&bD, but they are not always sufficient to comply with Article 25 GDPR

As stated by the EDPB, "PETs in themselves do not necessarily cover the obligations of Article 25."[24] This view is aligned with academics who rebut the claim that DPbD&bD is synonymous with formal PETs.[25] According to some scholars, DPbD&bD could more broadly serve as a tool for striking a fair balance between a wide array of rights and for openly discussing which rights and risks should be prioritized over others.[26] That is possibly the reason why the EDPB states that PETs should be seen only as one of the many means that can help achieve DPbD&bD.

The EU Agency for Cybersecurity's Ad Hoc Working Group (AHWG) on Data Protection Engineering seeks to analyze available or emerging technologies and techniques on engineering data protection principles (as stipulated by the GDPR) into practice. Its work — such as its recent "Engineering Personal Data Sharing" report — includes a focus on emerging technologies and a shift from PETs to design strategies, which may be helpful in understanding the role of PETs as an indicative solution and not as an end in itself.[27] According to Professor Hoepman, PETs are mainly

relevant after the controller has started developing a system, whereas privacy design strategies "translate vague legal norms in concrete design requirements [...] forcing one to make fundamental design choices early on."[28] PETs, nevertheless, if the context allows, can contribute to the correct implementation of Article 25 GDPR.

The EDPB guidelines on DPbD&bD ("EDPB Guidelines") do not specify which privacy engineering methods or PETs could reach the desired level of compliance with Article 25 GDPR. Thus, the burden for deciding lies, for the time being, with individual DPAs, who assess controller and processor PETs implementations on a case-by-case basis. Section 3.2 of this Report, below, will explore the limited extent to which DPA decisions on privacy preservation in online ecosystems are linked with the use of specific PETs, as regulators have devoted more efforts to clarifying their position on the matter through guidance.

Further clarity on the interplay between the adoption of PETs and DPbD&bD may come in the form of the upcoming EDPB guidelines on anonymization and pseudonymization.[29] The EDPB guidelines should consist of a review of the 9-year-old guidelines from the Article 29 Working Party, with the potential to bridge the conceptual and practical gaps between DPbD&bD and PETs.[30] Recently, the UK Information Commissioner's Office (ICO) has published draft guidance on PETs and how they map out vis-à-vis Article 25 and other provisions of the GDPR.[31] As the EU legislator is starting to reserve a spot for PETs in new regulatory initiatives, the time is ripe for the EDPB to step in and provide much needed clarity for public and private bodies that intend to use PETs as a key GDPR compliance tool.[32]

2. UNDERSTANDING TRENDS IN THE ENFORCEMENT OF DATA PROTECTION BY DESIGN AND BY DEFAULT OBLIGATIONS

This section will break down the legal obligations in Article 25 GDPR through analyzing enforcement actions from DPAs and Courts. First, Subsection 2.1. will "decode" key elements of Article 25, namely the role of the controller, the qualified nature of the obligation, the concept of appropriate TOMs, the time in which they should be applied, and the requirement of effectiveness. Then, we will analyze the first two paragraphs of Article 25 separately since they impose different obligations on the controller. The analysis will demonstrate that the two obligations differ in purpose and scope of application. With regards to the first paragraph of Article 25, which is about data protection by design, Subsection 2.2 will analyze its purpose and how it must consider individuals' rights and freedoms and general data protection principles. In Subsection 2.3 we will focus on the second paragraph of Article 25, referring to data protection by default. Finally, Subsection 2.4 will explore the divergent practice emerging in relation to compensation for non-material damage for breaches of the DPbD&bD obligations.

A decision from the Irish DPA illustrates the importance of analyzing the above elements separately and demonstrates the complexity and multi-layered applicability of Article 25 GDPR.

Case IE1: Default settings that make children's contact details publicly available are unlawful[33]

In September 2020, the Irish DPA (Data Protection Commission, or "DPC") initiated an investigation into the Instagram service, owned by Facebook Ireland Limited (FB), currently known as Meta Platforms, Inc. The investigation focused on:

- The processing of children's personal data when they switched to a "business account" feature, as they were required to display additional contact details on their profile page. Critically, FB was not applying any age restrictions in that context, so any child user could choose to have a business account; and
- The default setting of new business accounts being set to "public" unless changed to "private."

Following a procedure that involved a binding opinion of the EDPB,[34] the DPC determined that Articles 24 (Responsibility of the controller), 25 (DPbD&bD), and 35 (Data Protection Impact Assessment) of the GDPR require accounting for the nature, scope, context, and purposes of the processing. For the DPC, the *nature of the processing* involved the processing of the contact details and the public-by-default processing. Thus, it analyzed the scope, context, and purposes with regard to these two distinct operations. The *scope of the processing* of contact details and the public-by-default feature was considered very extensive, as it could reach an indefinite and unrestricted audience. The *context of the processing* of child users' contact details involved no age restrictions and mandatory publication until the opt-out option was introduced in 2019, whereas the public-by-default feature sought to maximize user engagement without acknowledging that it is possible for users to "seek, discover and connect on Instagram without also producing content for wider public consumption." Lastly, the DPC considered the *purposes of processing* for both of the settings as described by FB (service provision) to be simplistic and "open ended," lacking the level of transparency towards data subjects required under the GDPR.

Regarding *risks* to the rights and freedoms of natural persons, the DPC sought to clarify that risks are, by nature, only a possibility and are not synonymous with "damages" or "harms" but rather the *potential for damages or harms* and that Articles 24 and 25 refer to "potential risks," "possible harms," and "exposure to danger." The DPC determined that FB should have tackled risks, such as potential online sexual offenses, child abuse, or exploitation — which could be considered inherent to the service — as well as the use of accurate email and phone contact details for fraud and impersonation purposes. Overall, for the DPC, *both types of processing pose "high risks" to the rights and freedoms of child users.*

The DPC noted that FB's *measures* of restricting direct messages to minors and other steps to address the risks of grooming, child trafficking, and child exploitation did not meet the requirements of Articles 24 and 25 GDPR given that they focused on resolving issues rather than preventing them. Moreover, it stressed FB's measures concerning the publication of child users' contact details and the public-by-default setting sought to diminish the risks, but the way in which they were implemented was deficient. This deficiency stemmed from how FB did not impose any control or restriction on who could access and use child users' information, while it incentivized such users to switch to a business account without making it clear to them that their contact details would be made publicly available. Concerning the public-by-default setting, the DPC found that child users had no control over who obtained access to their contact details, and both they and their legal guardians were not given sufficient information about how they could protect themselves against dangerous individuals getting in touch.

Case IE1, continued

Following the aforementioned analysis, the DPC established a breach of Article 25 GDPR in relation to child users' contact details and the public-by-default setting, also linked to an infringement of the data minimization principle under Article 5(1)(c) GDPR. *Although acknowledging that Articles 24 and 25 GDPR give the controller some margin to choose the appropriate measures and that controllers may not be obliged to enforce specific one-size-fits-all measures, the DPC stated that controllers' choices should reflect and respect all the relevant GDPR provisions*. It sanctioned FB to pay 405M EUR for a total of 10 administrative fines, three of which related to FB's breaches of Articles 25(1) and 25(2) and DPbD&bD obligations. The latter administrative fines amounted to 75M EUR.

2.1. First steps in assessing Article 25 compliance: context of processing, risks, and the TOMs appropriate to them

Article 25 integrates two distinct obligations for controllers. They have to implement appropriate TOMs, both at the time of the determination of the means for processing and at the time of the processing itself, that ensure effective data protection by design (under paragraph 1) and data protection by default (under paragraph 2). These obligations build on Article 32 ("security of processing") and on provisions related to accountability like Article 24 ("responsibility of the controller") and Article 5(2) ("accountability"), as well as the other overarching data protection principles under Article 5, and ensuring the rights of the data subject under Chapter III.

a. The controller is responsible to comply with the DPbD&bD obligations, but the relationship with processors is under increased scrutiny

According to Article 25 GDPR, only controllers are responsible for applying measures that ensure DPbD&bD.[35] Even when they decide to use processors, Article 28(1) GDPR stipulates that controllers should choose processors who provide "sufficient guarantees to implement appropriate technical and organizational measures" for GDPR compliance. On the other hand, Recital 78 GDPR states that producers of products, services, and applications are only encouraged, but not obliged, to implement DPbD&bD measures when developing and designing such products, services, and applications.[36] This means that the controller retains full responsibility for compliance with Article 25 GDPR. However, the relationship between the controller and the processor is subject to intense scrutiny for DPbD&bD purposes, with the actions of processors having consequences for the liability of controllers. For instance, in the case below, the unilateral actions of the processor ensured that the controller was not found in breach of Article 25.

Case BE1: The website owner deploying a mandatory Microsoft login remains as the controller and responsible for ensuring DPbD&bD[37]

The Federal Public Service of Finance (FPS Finance) in Brussels granted free access to tax-related documents and guidelines via an online repository called FisconetPlus. In 2018, the repository moved and was hosted on the local government's website. Citizens could still access all the available material, but they were now obliged to create a Microsoft account to do so. FPS Finance argued that at the time of the choice to integrate Microsoft's login solution, it was not mandatory to log in with a Microsoft account to access the repository. However, according to FPS Finance, Microsoft then unilaterally made authentication through its solution mandatory for security reasons, *which meant that FPS Finance could not be accused of a violation of Article 25 GDPR*. Pursuant to a data subject's complaint and its Inspection Service's investigation, the Belgian DPA's Litigation Chamber decided that FPS Finance entered into the contractual agreement with Microsoft that required citizens to use a Microsoft account (anonymous or not) to access FPS Finance's services. *Thus, it is FPS who opts for Microsoft's digital services and products and thus determines the means of processing* (para 101)*, which qualifies FPS as the controller and, therefore, makes it responsible for the implementation of DPbD&bD.*

DPAs have often found that, in order to ensure effective DPbD&bD, the controller should define the role of its processors, establish the parameters of the processing from the outset — such as establishing retention periods, inform them of their obligations, and have a binding and sufficiently detailed contract.

Case IT1: Municipalities should inform their service providers about processing duties [38]

The Italian DPA (Garante) initiated an investigation concerning parking meters in Rome. Of particular concern was the fact that drivers had to enter the license plate of their vehicle to obtain a parking ticket. The system — which was collecting information such as the starting and ending times of the parking, the amount due, and the license plate of the car — was operated by the company "Atac s.p.a." on behalf of the Municipality of Rome. After an investigation triggered by a report that accused the municipality of unlawfully processing drivers' personal data, the Garante determined that the controller (the municipality) infringed Article 25 GDPR for not informing private companies acting as processors about how and for how long they should process personal data and for not defining their role under a written agreement. The Garante issued an 800,000 EUR fine and ordered the municipality to implement system log registration and monitoring, as well as to define and honor appropriate data storage limitation periods.

The EDPB Guidelines on DPbD&bD note that processors' operations should be regularly reviewed and assessed by the controller to ensure compliance with DPbD&bD at all times.[39] This is acutely reflected in two enforcement actions from the Polish DPA.

Case PL1: Neglectful oversight of a processor leading to data breaches[40]

An energy provider, Fortum Marketing and Sales Polska S.A (Fortum), failed to monitor the processing activities of its processor, PIKA Spółka z o.o. (PIKA). The latter did not implement appropriate security measures, and third parties accessed and extracted personal data of 137,314 customers. According to the Polish DPA (UODO), Fortum was obligated — and failed — to apply and review TOMs that were applied by its processor. The UODO determined that Fortum was more interested in increasing the efficiency of its systems than in ensuring an appropriate level of security of personal data. Failure to carry out audits, including inspections, of the processor represents a violation of Article 25(1) GDPR since this provision obligates controllers to implement appropriate measures, not only when determining the processing methods but also during the processing itself. Fortum did not supervise at any stage the implementation of the new system by PIKA and whether the latter applied generally accepted security standards.

In a similar case in Poland (**Case PL2**), the DPA found that ID Finance Sp. z o.o, a loan company, failed to regularly verify the methods used by its processor to detect security vulnerabilities. Due to a vulnerability, personal data of 140,699 clients was stolen and the UODO issued a fine of PLN 1,069,850 (approximately 250,000 EUR) for the violation of Article 25(1) GDPR.[41]

b. The DPbD&bD obligations are context-dependent, weighing in the state-of-the-art of technology, the cost of implementation, the nature of the processing, and the likelihood of risks

From the first lines of Article 25(1) we learn the contextual factors that controllers should bear in mind when implementing TOMs. Therefore, Article 25(1) GDPR's risk-based approach and the phrase "taking into account" in the same provision could be understood as requiring controllers to engage in a thought exercise and inquire into the different elements associated with the processing that may trigger risks to the rights and freedoms of individuals before selecting appropriate and effective TOMs.[42]

The role of a Data Protection Impact Assessment (DPIA) under Article 35 GDPR in this context could be essential, as demonstrated by several enforcement actions from DPAs under Article 25. However, even if DPIAs can be an integral part of DPbD&bD, a DPIA is only required in certain circumstances,[43] whereas the DPbD&bD is a broader concept that is central to GDPR compliance.[44]

Case FI1: Employee location data processing during requires a DPIA[45]

A company was collecting location data from its employees' vehicle GPS trackers during their working hours without carrying out a DPIA as mandated by Article 35 GDPR. The Finnish DPA (Office of the Data Protection Ombudsman) determined that since the company was systematically monitoring employees' location, the risk to their rights was high, and a DPIA was thus necessary. The DPA noted that the controller did not implement sufficient TOMs, neither for determining how the processing of employee location data is to be carried out nor for the processing itself, to ensure that the principles of the GDPR are incorporated and that the fairness of the processing can be ensured and demonstrated. A breach of Article 25 was found. The DPA sanctioned the company with a 16,000 EUR fine.

The four factors that frame data protection by design as a qualified obligation under Article 25(1) are analyzed below.

- ***State-of-the-art of technology:*** According to the EDPB Guidelines, when choosing appropriate TOMs, controllers should consider the current progress in technology that is available on the market. This means that controllers should be continuously up-to-date on technical and organizational measures and technological developments and leverage them in their GDPR compliance.[46]

Case FI2: Lack of state-of-the-art measures can lead to heavy fines and bankruptcy:[47]

Vastaamo Oy's, a psychotherapy company, suffered two data breaches involving its patient records and was blackmailed by the hacker. Later on, approximately 15,000 patients also received threats from the hacker, and some of their health records were circulated on the internet. Following these events, the company declared bankruptcy in 2021, as the Finnish Data Protection Ombudsman concluded there were breaches of Articles 5(1)(f), 24(1), 25(1), 32(1), and 32(2) GDPR. The DPA determined that the server where the company hosted its electronic health records was not supported by best practices and current security methods and was thus prone to attacks. Most importantly, the server lacked firewall protection and sufficient root user authentication. The DPA decided to impose a total fine of 608,000 EUR.

Case IE2, which we analyze in more detail below in Section 2.1.e. also offers important insights about how the Irish DPC considers the "state-of-the-art" criterion in controller's choice of TOMs.

- ***Cost of implementation:*** According to the EDPB Guidelines, controllers should consider the cost of implementation of TOMs, but the controller cannot present an incapacity to bear high costs as an excuse for non-compliance with Article 25(1).[48] Despite the fact that both Articles 25 and 32 refer to the cost of implementation of specific TOMs as one of the factors that controllers should consider when selecting and implementing measures, *DPAs do not seem sympathetic to cost-based justification for not deploying effective TOMs*.

Case IT2: High costs do not justify keeping unencrypted whistleblower data[49]

The Italian Garante initiated an investigation into Aeroporto Guglielmo Marconi di Bologna S.p.a's whistleblowing application called "WB Confidential." Among other shortcomings, the Garante determined that the Company was not encrypting the data that it was obtaining from whistleblowers and then storing, which resulted in an insufficient level of security and breaches of Articles 5(1)(f), 24, 25, and 32 GDPR. The DPA rejected the defendant's arguments that deploying encryption would be too costly and that access was limited to technicians appointed by the processor that managed the application, thereby issuing a 40,000 EUR fine.

- ***Nature, scope, context, and purposes of processing:*** Controllers should also consider the nature, scope, context, and purposes of processing when choosing TOMs under Article 25(1) GDPR. According to the EDPB Guidelines, "the concept of nature can be understood as the inherent characteristics of the processing. The scope refers to the size and range of the processing. The context relates to the circumstances of the processing, which may influence the expectations of the data subject, while the purpose pertains to the aims of the processing."[50] DPAs are more prone to find breaches of Article 25(1) GDPR where the controller omits robust TOMs in processing activities involving a high number of data subjects, sensitive categories of data, or opaque automated practices, as several case studies we have analyzed above show. **Cases IE1** and **IE2** are particularly illustrative of how the Irish DPC evaluates these elements in a very detailed fashion and offer controllers detailed analysis on how to use these four factors when organizing processing activities.

- ***Risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing:*** According to the EDPB Guidelines, "when performing the risk analysis for compliance with Articles 24 and 25 the controller has to identify the risks and determine their likelihood and severity."[51] Once more, the EDPB Guidelines on DPIAs may be useful in such an exercise, as they offer detailed risk assessment criteria for data processing operations.[52]

Case PL3: Light risk assessments may lead the controller to not consider the right TOMs[53]

A waste management company disclosed to unauthorized recipients a list containing addresses of people that were in quarantine, either due to crossing the country border or a confirmed SARS-CoV-2 infection. In its risk assessment, the company had identified the threat of theft or removal of data by employees or associates. For this reason, it required its employees to comply with specific procedures, sign confidentiality agreements, and complete data protection training while also equipping its data storage facilities and systems with anti-theft alarms and encryption. However, the Polish UODO indicated that these measures were general in nature and did not address the scenario of data leakage carried out by authorized employees (e.g., an authorized person leaving printed address lists on their desks or taking and sharing pictures of such lists). Thus, the UODO concluded that the controller should have taken into account both the specific nature of the processed data and the human factor, which is one of the sources of risk in the processing of personal data. By failing to apply appropriate measures and regularly test existing ones, the controller violated Article 25(1) GDPR. The UODO issued a reprimand and ordered the company to inform data subjects about the breach.

c. TOMs must be comprehensive: organizational measures, like training and frequent vulnerability tests, matter as much as technical measures, like encryption

Article 25 GDPR refers to "technical and organizational measures" for the implementation of data protection principles and explicitly mentions pseudonymization as an indicative technical measure.[54] Other examples are listed in Recital 78 GDPR. The EDPB Guidelines further note that measures should be understood in a broad sense "as any method or means that a controller may employ in the processing" as long as they are appropriate to reach their intended goal.[55] The Spanish DPA (AEPD) offers more detailed guidance with practical examples regarding both the strategy for data collection (such as anonymization, encryption, isolation, and separation of data) and the further processing of personal data. The latter includes dynamic visualization of privacy policies, selection of credentials, informed consent, evaluation of DPIAs, access controls, and management of obligations.[56]

The enforcement cases we found and that we outline in this section mainly showcase the role of organizational measures. This contradicts the perception that DPbD&bD is primarily linked to technical measures and highlights the importance of finding an appropriate measure for the specific processing *in concreto* and not in abstract.

The EDPB Guidelines note that standards, best practices, and codes of conduct can be helpful, but the controller is still obliged to assess their appropriateness for the particular processing in question.[57] With regards to the requirement of *appropriateness*, it is argued that the controller bears an "obligation of result": the measures may be of any kind, but they have to achieve their intended protective purpose.[58] This obligation is why the appropriateness of the measures is closely linked with their effectiveness and also why certain DPAs — like the Irish DPC in Case IE1 — tend to associate implemented measures with identified risks and does not determine in abstract terms whether a measure is sufficient and appropriate.[59] The Catalan DPA (APDCAT), in its recent Guide for Developers, noted that effective data protection by design and by default requires developers to consider the context in which their product will be used in order to configure it with appropriate guarantees.[60]

Case PL4: A risk assessment and targeted measures, such as vulnerability tests, could have prevented leaks of data related to admission at university[61]

An unauthorized third party gained access to certain Warsaw University of Technology students', candidates', and lecturers' personal data. The software tools that the university was using to process admission applications were linked to a database that contained personal data. The third-party managed to access the database using the credentials of a lecturer, placed a file that allowed for data exfiltration, and downloaded files containing personal data. The Polish UODO imposed a fine of PLN 45,000 (approximately 9,900 EUR) after concluding that the University had violated Articles 5(1)(f), 5(2), 24(1), 25(1), 32(1), and 32(2) of the GDPR. More specifically, the DPA found that:

The passwords were stored in the form of an MD5 hash without any additional security measures, whereas the controller should have used an additional random parameter of the encryption function.

The university did not perform tests or formal risk assessments on the application in order to detect system vulnerabilities to attacks from the public network. The UODO noted that using antivirus tools, regularly updating software, and monitoring activity through logs were insufficient measures and that *the controller's risk assessment should have considered the real possibilities of the attack, social engineering methods, and state-of-the-art*. The assessment of whether the adopted or planned measures were appropriate should have been done both at the design stage and at a later level.

Case PL5: Multi-factor authentication as a way to avoid phishing scams[62]

Morele.net reported a data breach to the Polish UODO. In this case, an unauthorized person gained access to the customer database of certain online stores of the controller. For the UODO, the company violated Articles 5(1)(f) and 25(1) GDPR due to ineffective authentication procedures — based on simple username and password credentials — that did not prevent unauthorized access. The DPA explained that access control and secure authentication are basic security measures that the controller should have implemented. It furthermore pointed to relevant European Union Agency for Cybersecurity (ENISA) guidance and other resources to recommend the use of a two-factor authentication mechanism for systems involving access to personal data.[63] The resources on state-of-the-art secure authentication procedures quoted by the DPA indicate that the *selection of the appropriate authentication measure should be preceded by a risk analysis and be subject to constant reviews*, which the company failed to carry out. For the DPA, the company's failures amounted to an infringement of Articles 25(1) and 32 GDPR, and so it decided to impose a fine of PLN 2,830,410 (approximately 660,000 EUR).

On a judicial appeal from the defendant, the Provincial Administrative Court of Warsaw upheld the DPA's decision without going into detail in its reasoning.[64]

In addition, according to DPAs, technical measures could be insufficient if organizations do not provide staff with appropriate security and data handling training. However, no employee can replace the controller in the performance of its duties, despite the workings of Article 29 GDPR. This means that training by itself should be seen as a weak DPbD&bD measure that should be complemented by additional measures.

Case PL6: Attaining appropriate security is an ongoing process[65]

A probation officer of the District Court in Zgierz (Poland) lost an unencrypted USB stick that contained personal data — including sensitive data — of 400 persons subject to probation. The President of the District Court reported the loss of the USB stick, and the DPA determined that: (1) the training of employees and the technical measures that the controller instructed them to apply were not enough since employees cannot replace the controller in the performance of its tasks; (2) the controller should not use unsecured portable storage media at all, and additional measures such as encryption should have been implemented; and (3) the controller was using ad hoc testing instead of regular testing that could verify the effectiveness of the implemented security measures. Hence, the DPA found an infringement of Article 25(1) GDPR and of the integrity and confidentiality principle under Article 5(1)(f) GDPR, thereby imposing a fine of PLN 10,000 (approximately 2,150 EUR) on the District Court.

Other cases show the importance of combining TOMs for a robust implementation of DPbD&bD under Article 25 GDPR.

Case HU1: Lack of internal email-handling rules for employees is an Article 25 breach[66]

A former employee of an unnamed company notified the Hungarian DPA (NAIH) that during the period of his incapacity for work due to sickness, his desk and computer equipment were used and someone had accessed his email account and physical documents. The NAIH noted that the employer bears the responsibility of setting up an internal policy that ensures the personal data of employees will not be unlawfully processed. For the DPA, this responsibility could be ensured by internal rules that define whether the employee can use the email account or devices for private purposes and include provisions for backing up, storing, and deactivating email accounts, among others. The DPA determined that the controller did not have any such rules in place in the form of technical and/or organizational measures concerning the use of e-mail accounts and computer equipment and was therefore violating Article 25 GDPR. The regulator issued a fine of approximately 2,860 EUR.

d. TOMs must be in place before and during the processing

The controller shall, *both at the time of the determination of the means for processing and at the time of the processing itself*, implement appropriate TOMs. This is relevant for both paragraphs (1) and (2) of Article 25 GDPR.[67] In practice, and as we have seen with **Cases PL1** and **PL5**, controllers should consider DPbD&bD throughout the data management cycle.[68] As the EDPB Guidelines note, the controller will benefit "from a cost-benefit perspective," taking into account the correct implementation of data protection principles sooner rather than later. Moreover, the controller has a continuous obligation to maintain DPbD&bD by re-evaluating the adopted measures.[69] Considering the enforcement actions that we have analyzed, DPAs across Europe seem to be aligned with the EDPB's views.

Case FI3: Channels for processing data access and erasure requests must be functional at all times[70]

The Finnish Data Protection Ombudsman received complaints about publishing company Otavamedia Oy regarding infringements of access rights under Article 15 GDPR, amongst others (see Section 2.3 below). In this case, the company did not respond to certain access requests due to a technical error in its systems that lasted seven months. For the DPA, the controller allowed technical errors to occur since it did not regularly check the functionality of its emailing systems. In any case, the mere establishment of a contact channel aimed at registered users is not sufficient on its own, but it must also be functional at all times. Since the controller neglected to check the functionality of the system it used to receive data subjects' requests, it violated Articles 12, 15, 17, and 25(1) of the GDPR. As a result, the DPA issued a fine of 85,000 EUR.

e. TOMs need to be effective in preventing the materialization of risks

Article 25 GDPR aims at safeguarding data protection principles and data subjects' rights "in an effective manner." The EDPB Guidelines note that "effectiveness is at the heart of the concept of data protection by design" and explain the two consequences of this conclusion: 1) the controller is not obliged to implement any prescribed measures since the appropriateness of them will be contextual, as seen in **Case PL4** above; and 2) the controller has to *demonstrate* that the measures have an actual effect and are not "generic," which can be assessed either by using key performance indicators such as quantitative or qualitative metrics or by providing the rationale behind the implemented measures.[71] *This means that the TOMs chosen by controllers must not only be appropriate to the identified risks but must also effectively prevent the occurrence of GDPR violations*.

Case IE2: Social media user searching tools made the platform vulnerable to data brokers and data scrapers[72]

The Irish DPC commenced an inquiry in April 2021 after media reports that a Facebook dataset containing users' personal data was made available on the internet. Meta Platforms Ireland Limited (Meta), the owner of the Facebook social media network (FB), used specific data processing tools to allow users to find their friends' contacts on the network by entering their phone numbers or email addresses. The DPC's investigation revealed that the dataset concerned 533M Facebook users. The DPC found infringements of Articles 25(1) and 25(2) of the GDPR. We explore the latter in Section 2.3 below.

To tackle the risk of malicious data scrapers, Meta had put in place TOMs, like rate limiting[73], and a dedicated team to monitor, prevent, and mitigate data scraping, which Meta argued constituted industry best practices.

In its decision, the DPC followed the EDPB in noting that **effectiveness is at the heart of the concept of data protection by design**, meaning that the adopted measures should be designed to be robust and the controller capable to scale them up. Thus, the DPC proposed certain indicative measures that were viable options that Meta failed to adopt, taking into account the scope of Meta's large-scale processing and the severe risk of malicious actors acquiring personal data due to the higher likelihood that random numbers and email addresses would match real FB users. For the DPC, sufficient measures would, inter alia, prevent exact matches following a lookup — instead returning a selection of profile near matches — and detect bot action.

According to the regulator, Meta failed to implement appropriate measures according to Article 25(1) GDPR that could safeguard the purpose limitation and integrity and confidentiality principles under Article 5(1)(b) and Article5(1)(f) GDPR. This is because FB's contact searching tools allowed bad actors to create a dataset for purposes other than finding profiles of FB users and to discover the identity of FB users who own random phone numbers or email addresses. The DPC issued a 265M EUR fine, of which 150M were due to an infringement of Article 25(1) GDPR.

In Poland, the UODO has focused heavily on enforcing DPbD&bD requirements where the controller did not — either directly or through its processors — implement enough TOMs to effectively prevent data breaches.

Case PL7: Outdated software opens the door to attackers[74]

A healthcare provider notified the Polish UODO about a data breach it suffered concerning personal data of employees, clients, and patients. Third parties bypassed the security of the company's IT system, gained access to personal data, and then, using encryption malware, deactivated the existing antivirus protection, encrypted the dataset, and prevented the company from accessing the system. For the UODO, the controller did not implement appropriate TOMs to ensure that data was processed securely in its IT systems. The company should have ensured an appropriate level of data security and alignment with Article 5(1)(f) GDPR by relying on the manufacturer's technical support, configuring its IT systems, and conducting a regular evaluation and testing of the effectiveness of its TOMs.

The DPA referred to the judgment of September 3, 2020, file ref. II SA/Wa 2559/19 of the Provincial Administrative Court in Warsaw that stated companies should ensure continuous monitoring of the level of threats and accountability regarding the adequacy of their security measures.[75] Moreover, they should tweak their measures and procedures on an ongoing basis to adjust them to the identified risks to the rights and freedoms of individuals. The regulator decided to issue a reprimand since the breach concerned as a one-time event and was not a systematic unlawful act or omission on the part of the controller.

2.2. Data protection principles and the rights of the data subject must be ensured "by design"

As the EDPB Guidelines have clarified, the TOMs that controllers must adopt under Article 25(1) GDPR should aim to safeguard 1) general data protection principles under Article 5 GDPR, 2) data subjects' rights found in Articles 12 through 22 GDPR, and 3) data subjects' freedoms found in Recitals 4 and the EU Charter of Fundamental Rights (EUCFR).[76] We thus highlight that controllers must think beyond ensuring compliance with data protection principles and rules when implementing PDbD&bD, and should also consider other equally important fundamental rights, such as respect for private and family life, confidentiality of communications, and freedom of thought, expression, and information.

a. Controllers often jointly breach DPbD&bD and Article 5 principles, like data minimization

Article 25(1) refers to the principles found in Article 5 of the GDPR. We will analyze enforcement cases involving breaches of each one of the principles in connection with Article 25(1) GDPR, although we stress DPAs often find infringements of Article 25(1) without references to any principles under Article 5. On the other hand, we note that in many instances DPAs and courts refer to *breaches of multiple Article 5 principles* as a result of, or in relation to, Article 25(1) infringements while not necessarily elaborating in a detailed manner about why such principles were overlooked by the controller.

Case IT3: Financial aid management must respect data protection principles[77]

The Italian Garante found that the Italian National Institute for Social Security (INPS), while managing financial aid for citizens affected by the Covid-19 pandemic, kept data of individuals who were no longer aid beneficiaries and acquired personal data from external sources of uncertain quality. According to the DPA, these practices violated the principles of lawfulness, data minimization, and accuracy under Article 5 GDPR. The Garante ruled that the INPS was also not in compliance with Article 25(1) GDPR and issued corrective measures, including deletion of the unlawfully processed personal data and a fine of 300,000 EUR.

In other cases, DPAs refer to DPbD&bD-linked Article 5 GDPR breaches more generally, without identifying which exact principle was violated.

Case RO1: Surveillance system for private purposes[78]

An apartment building owners association was sanctioned by the Romanian DPA (ANSPDCP) for the illegal processing of the image of a natural person. The image was captured by the association's CCTV surveillance system and was displayed in the building's CCTV notice. For the DPA, this action breached data protection principles under Article 5 GDPR, and the controller also failed to implement appropriate TOMs in accordance with Articles 25 and 32 GDPR. The DPA issued a 500 EUR fine and ordered the association to implement specific TOMs, including the deactivation of remote access to the CCTV system and the limitation of access to a specified number of people with clear processing instructions.

i. Lawfulness, Transparency, and Fairness

***Lawfulness**:* According to the EDPB Guidelines, compliance with data protection by design entails that the controller identifies a valid legal basis for the processing of personal data and respects the principle of lawfulness. This compliance also requires that data processing respects all applicable legal requirements, such as the ones derived from sectoral and consumer protection laws.[79] Key by-design and default elements for lawfulness that the EDPB has endorsed and that are reflected in a number of DPA enforcement actions under Article 25(1) GDPR include:[80]

- Where the processing relies on *consent*, it must be specific, informed, unambiguous, and freely given. DPA case-law enforcing Article 25 GDPR also indicates that organizations should ensure they do not rely on manipulative techniques to obtain user consent for data processing given that deceptive design patterns ("dark patterns") violate the principle of lawfulness along with DPbD&bD.

Case IT4: Mandatory consent for marketing purposes is unlawful and breaches data protection by design[81]

An Italian electronic communications operator (Iliad Italian SpA) obliged consumers to "tick" a box declaring that they had read and accepted the company's terms and conditions and privacy policy before they could have their SIM cards activated. The Italian DPA found that such practice was contrary to Articles 25 and 5(1)(a) GDPR, as consent for processing for promotional purposes was made mandatory by the company in the sign-up process. This mandatory "consent" was required despite the fact that such processing did not occur in practice, nor was foreseen by the controller. Given the lack of consequences for consumers and that the company was acting unintentionally and adopted measures in order to address the detected infringements, the Garante merely issued a warning.

Case BE2: Placement of non-essential cookies requires opt-in consent[82]

The Belgian DPA initiated an investigation into Roularta Media Group, the controller of Belgian media websites "www.knack.be" and "www.levif.be," on its use of non-essential cookies. The DPA noted that the company was using pre-ticked consent boxes, with the cookies of third parties ("partner companies") marked as "active" by default. Such placement of cookies was contrary to provisions of the ePrivacy Directive and the GDPR. As consent for non-essential cookie placement was mandatory under the Belgian law transposing Article 5 of the ePrivacy Directive, the controller should have sought website visitors' affirmative and active consent. The controller's practices thus breached Articles 4(11), 6(1)(a), and 7(1) GDPR, as the consent that the controller claimed to have obtained for the placement of such cookies was invalid. The DPA issued a 50,000 EUR fine and further ordered the controller to bring its processing of personal data into compliance with the GDPR within three months.

Case IS1: Access to bank account requires prior consent from the account holder[83]

A bank allowed a legal guardian to have continuing access to a bank account opened by their daughter even after she became an adult. For the Icelandic DPA (Persónuvernd), the bank was obliged to ensure that access to the bank account is granted only to authorized people based on the holder's consent, such as persons with appropriate power of attorney, which the legal guardian lacked. As such, Persónuvernd found breaches of both Articles 5(1)(a) and 25 GDPR.

Case IT17: Obtaining consent through "dark patterns" breaches DPbD[84]

The Garante imposed a 300,000 euro fine to a digital marketing services company for tricking users to consent to the processing of their data by using "dark patterns" on its portals.

Necessity: the processing must be "necessary and unconditional" for the purpose to be lawful.

Case FI4: Using a teaching software is not necessary for the fulfillment of public tasks[85]

A complainant brought to the attention of the Finnish Data Protection Ombudsman the use of Google Workspace for Education by public schools. The DPA noted that schools do not need to use an electronic teaching program to fulfill statutory obligations concerning education and thus, the controller (local municipality) was unlawfully processing students' personal data since the "legal obligation" ground under Article 6(1)(c) GDPR could not be used as a legal basis. The DPA noted that voluntary unilateral commitments and public-private partnerships, where data is processed more extensively than required by law, do not fall within the scope of the basis for processing personal data related to a statutory task. The DPA also noted that when a school uses free programs in education, it should first properly and wholly evaluate applying Article 25 GDPR.

***Relevance*:** the correct legal basis shall be applied to the processing.

Case IT5: Access to health data for purposes other than healthcare needs a legal basis[86]

The Italian Garante determined that health personnel working at the Central Friuli University Health Authority (ASUFC) had unrestricted access to the health records of persons who were not treated by them or whose treatment did not require unlimited access. Furthermore, the staff had access to health records to support organizational processes, ensure regulatory compliance, and provide critical review and possible improvement of care pathways. The Garante found a violation of Articles 5(1)(a), 9(1), and 25 GDPR, notably because healthcare professionals were processing health data for secondary purposes without a proper lawful ground.[87] Therefore, the Garante issued a fine of 70,000 EUR.

Transparency: the controller must be clear and transparent to the data subject about how they will collect, use, and share personal data, which is also reflected in Recital 60 GDPR. Key design and default elements for transparency that the EDPB has endorsed and that were validated and further detailed by European DPA enforcement actions include:

- ***Contextual, comprehensible, and multi-channeled*** information. The former requires the controller to provide information to data subjects about the processing of their personal data at the relevant time and in the appropriate form, as set out in Articles 12 through 14 GDPR.

Case BE1: Article 25 could be applied despite the absence of processing[88]

In this case — which we already explored above in Section 2.1.a. — the Belgian Federal Public Service of Finance (FPS) required citizens to create a Microsoft account in order to access tax-related documents. Microsoft's privacy policy included mandatory acceptance of tracking for advertising purposes. The Inspection Service of the Belgian DPA found that this practice had no legal basis under GDPR and asked FPS to stop requiring citizens to create a Microsoft account in order to access the repository. In response, FPS implemented temporary measures which allowed access to the database without requiring a Microsoft account or via an "anonymous" Microsoft account. However, the Inspection Service found that it was misleading to refer to the option of using Microsoft "anonymously" since cookies were placed in users' devices, and therefore users were given inaccurate and incomplete information concerning access possibilities and the placement of cookies, and FPS did not offer the most privacy-friendly approach (i.e., direct access to the database without identification). For the DPA, these amounted to breaches of Articles 5(1)(a), 5(1)(c), 12, 13(1)(f), 25(1), and 25(2) GDPR.

Interestingly, given that the complainants in the case had not actually logged in with a Microsoft account to access the repository, the Belgian DPA Litigation Chamber stressed that *legal protection via the DPA is only possible when an actual processing of personal data occurs and not when a data subject refuses a specific processing as a practice because they consider it to be inconsistent with their own rights* (para 109). *However, this does not mean that FPS cannot be held accountable under the GDPR by the DPA. On the contrary, Article 25 GDPR could be applied despite the absence of processing and of a violation of Article 5*.

It is interesting to compare this position from the Belgian DPA with the stances taken by its Irish and Spanish counterparts in two other cases related to identity verification requirements in the context of access requests under Article 15 GDPR (see **Cases IE3** and **ES1**). In contrast to decisions from the Austrian and Finnish DPAs (see **Cases AT2** and **FI5**[89]), the Belgian, Irish, and Spanish DPAs are all favorable to enforcing Article 25 GDPR against controllers whose planned but not yet implemented processing activities would breach GDPR principles and obligations.

Case IE3: ID checks in the context of access requests can breach the data minimization principle[90]

In a recent decision, the Irish DPC determined that Airbnb's requirement that the complainant verify their identity by way of submission of a copy of their photographic ID constituted an infringement of the principle of data minimization under Article 5(1)(c) GDPR. This decision was made despite the fact that the complainant refused to submit a copy of his ID document and used a different option for proving his identity to the controller.

Case ES1: Employment Agency fined 300,000 EUR for unnecessary identity verification[91]

A Dutch citizen who created an account with recruitment agency Michael Page filed a complaint with the Dutch DPA (Autoriteit Persoonsgegevens, or "AP") arguing that when she made an access request, the controller asked for her ID to fulfill her request, which she found to be unnecessary. The Dutch AP forwarded the case to the Spanish AEPD as the lead supervisory authority (Articles 4(16), 56(1) GDPR), since the company's legal department responsible for managing all access requests was based in Barcelona. The AEPD determined that the company's practice was legitimate to prevent unauthorized access to personal data. However, both the Portuguese (CNPD) and the German State of Berlin (BInBDI) DPAs filed reasoned objections as concerned supervisory authorities, in which they argued that, when handling a data subject's access request, controllers can only ask for additional information if the data subject's identity is contested. Both DPAs determined there were violations of Articles 12, 5(1)(c), and 25 GDPR. In particular, the CNPD noted that the contested measure does not protect applicants since the identification requirements increase the risks for data subjects (e.g., identity theft) and a less intrusive approach would suffice. Following this opposition, the AEPD re-examined the complaint and issued a fine of 300,000 EUR. More specifically, it found that the identity of the data subject was not contested, since the access request was made via the same email address associated with the individual's account with the company; the controller requested more information than necessary to verify the individual's identity; and the controller's identification procedure for handling access requests breached Article 25(1) GDPR, as it was not adapted to the context, risks, and purpose of the processing.

Accessibility: information shall be easily accessible for the data subject at all times, particularly when the data subjects are children or other vulnerable groups.[92]

Case FI6: Patients getting insufficient information[93]

After a patient complained that a medical clinic did not comply with a data access request under Article 15 GDPR, the Finnish Data Protection Ombudsman ruled that the controller failed to implement a system that would safeguard the principle of transparency as found in Article 5(1)(a) GDPR from the beginning of its operations. The DPA also found that *the controller's information was not easily accessible for data subjects, as it was not available and visible on all pages of the controller's website*. The controller could not explain to the DPA the steps it had taken to inform data subjects about its processing, and so the DPA found infringements of Articles 25(1), 5(1)(a), 12(1-4), 13(1-2), and 15(1-3) GDPR. The DPA issued a 5,000 EUR fine and an order for the clinic to bring processing into compliance.

Fairness: According to the EDPB guidelines, "fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject."[94] The following decision incorporated most of the key design and default fairness elements that the EDPB proposed.

Case NO1: Automated grading using historical data is unfair[95]

The Norwegian DPA (Datatilsynet) provided some insight into how the fairness principle under Article 5(1)(a) GDPR, DPbD&bD, and automated decision-making interact, through its intention to order the International Baccalaureate Office (IB) to correct student grades because of unfair profiling, published in August 2020. Given the cancellation of exams during the COVID-19 pandemic, the IB decided to consider students' "school context" and "historical data" in the grading. Datatilsynet determined that the use of such factors in awarding grades was a violation of the fairness principle and led to inaccurate grading. Notably, the DPA observed that such grading did not reflect the students' individual academic level, rather potentially leading to discrimination based on the school they attended. The DPA also pointed to the fairness criteria identified by the EDPB in its DPbD&bD guidelines, stating that any processing of data, including cases of profiling such as the one at stake, should be non-discriminatory, ethical, and transparent, and consider power and information (im)balances. In this regard, Datatilsynet stated that the grading system did not correspond to students' reasonable expectations, who expected their grades to reflect their demonstrable academic achievements and the work they had put in, as well as the knowledge and skills they had attained.

ii. Purpose Limitation

In the cases we have analyzed, DPAs often found a violation of the purpose limitation principle under Article 5(1)(b) when the controller processed personal data for purposes that were incompatible with the one for which the data was initially collected. The compatibility test under Article 6(4) GDPR is quite strict, but controllers must follow it when they plan to process personal data for new purposes without using an additional lawful ground under Article 6(1) GDPR.[96] The EDPB Guidelines — along with a specific enforcement action from the Belgian DPA — have stressed that limiting further processing is a key design and default element along with others such as predetermination, specificity, purpose orientation, and necessity.[97]

Case BE3: Sending political messages to a complainants database is incompatible processing[98]

In 2019, a candidate for municipal elections in Belgium — who was also the mayor of the municipality at the time — sent a campaigning email to a citizen who five years prior used that very email address to complain to the municipality about public cleanliness. According to the Belgian DPA Litigation Chamber, the electoral candidate had been keeping a list of citizens that had contacted the municipality, even though the processing should have been limited to answering citizens' questions. For this reason, *the Belgian DPA considered the candidate to be the controller and not the municipality, as the candidate was processing citizens' data for his own purposes*. Moreover, the DPA found that the candidate's messages left all recipients' email addresses visible to each recipient. According to the DPA, the candidate's subsequent processing violated Article 5(1)(b) GDPR (purpose limitation principle), Articles 5(1)(a) and 6 GDPR (lawfulness of the processing), and Articles 25(1) and 25(2) on DPbD&bD. Given the above, the DPA decided to impose an administrative fine of 5,000 EUR on the candidate. It is notable that the decision refers to similar previous cases concerning unlawful data processing for electoral purposes, but this was the first case in which the Belgian DPA's Litigation Chamber considered Article 25 GDPR when imposing an administrative fine.

However, the DPA's decision was eventually overturned by the Brussels Appeals Court on appeal (**Case BE-CR-1**). The court considered that the DPA's decision lacked proper justification under Article 83 GDPR and was disproportionate. Therefore, it invalidated the DPA's decision and ordered it to pay the defendant's legal costs. According to the court, the DPA should have considered the non-deliberate nature of all infringements, including the breaches of Articles 5 and 25 GDPR.[99]

iii. Data Minimization

The text of Article 25(1) GDPR explicitly states that the controller should safeguard the data minimization principle under Article 5(1)(c) GDPR from the moment it determines the means of the processing. This obligation includes ensuring that the purpose of the processing could not reasonably be fulfilled by other less intrusive means.[100] According to the EDPB Guidelines, relevant DPA enforcement, and court rulings, key design and default data minimization practices may include the following elements, depending on the specific case:[101]

- ***Relevance and necessity:*** each personal data category should be relevant and necessary to pursue the purposes and processing operations in question. In this respect, DPAs tend to often detect — sometimes without extensive justification — that more data than necessary is being requested or processed by the controller. Some examples include a case of a bank which disclosed personal data of the payer to the beneficiary (**Case RO3**, which led to a fine of 130,000 EUR[102]), a case where job applicants were required to fill out a form stating extensive personal data (**Case FI7**, which resulted in a 12,500 EUR fine[103]), and a case of a housing company that was asking for health-related data from its clients (**Case FI5**, in which, the DPA issued only a warning given that no actual data collection occurred). However, in other cases, DPAs dig deeper in establishing a link between the breach of the data minimization principle and DPbD&bD.

Case IT6: Access to systems with different purposes must be segregated[104]

Following an Italian Court ruling, the Italian Garante sanctioned food delivery company Deliveroo for its rider ranking algorithm and its personal data management system. The DPA found that the communications between Deliveroo's customers and riders were stored in two different systems ("Atlas" and "Payments") and they were configured in a way that made it possible for authorized operators to simply move information from one system to the other. This functionality allowed operators to combine the data available in each system. Moreover, when passing through from the order management system to the communications management system and vice versa, operators had access to not only the data relating to the rider who managed a particular order, but also to information relating to all the other riders. When entering each system, operators could access data that was not necessary for the completion of a task such as replying to a customer's complaint. For example, when assessing requests for compensation, the operators who enter the "Payments" system could directly access all the details of the orders placed by each customer, which was not necessary for addressing an individual complaint. Also, the chat and email management system was structured in a way that allowed operators to access its content without restrictions. The Garante determined that Deliveroo failed to explain why the simultaneous access of operators to different systems, which resulted in the collection of a large quantity and variety of data, was necessary for providing Deliveroo's services and answering customers' complaints. Thus, the DPA found breaches of Articles 5(1)(c) and 25 GDPR, imposed a fine of 2,500,000 EUR, and issued a set of orders related to data minimization and PbD&bD that Deliveroo had to implement within 60 days.

DPA decisions in Belgium and Spain regarding the use of CCTV cameras and facial recognition systems are particularly illustrative of how closely regulators read into compliance with necessity and proportionality requirements and data protection by design. This relationship also seems to be facilitated by the fact that EDPB guidance on video devices set out clear and detailed requirements for controllers who wish to embed data protection into their surveillance systems.[105]

Case BE4: CCTV cameras recording public areas and others' property reveals lack of DPbD&bD[106]

A couple placed surveillance cameras on their property, which also captured footage of their neighbors' property and a public street. The neighbors asked for the cameras to be taken down and for the recordings not to be used. The Belgian DPA's Litigation Chamber stated that the defendants should have ensured proper TOMs to avoid capturing unnecessary footage when installing CCTV cameras. Moreover, the DPA found that the continuous filming should have been done with due care and restraint and the unlawful processing operations reveal that appropriate TOMs under Article 25(1) were missing. Given that the controllers changed the arrangement of the cameras after a police intervention and did not pursue commercial interests, the Litigation Chamber decided to issue a reprimand and a deterrent fine of 1,500 EUR.

Case ES2: Facial recognition system is not proportionate nor effective to prevent criminals from entering premises[107]

Mercadona, a supermarket chain, installed a video surveillance system with facial recognition features at its premises in order to detect and prevent the entrance of individuals who had previously been convicted for crimes related to the supermarket chain. The Spanish AEPD found that the controller had no legal basis under Spanish law to conduct such processing and that the personal data was not necessary, adequate, nor proportionate to the envisaged goal. There were also less intrusive measures to achieve the set goal — such as providing photographs of convicted people to the security personnel — and convicted persons could easily circumvent the system with a simple mask. The AEPD determined there was a breach of Article 5(1)(c) GDPR along with Article 25(1), for which the DPA imposed a 2,520,000 EUR fine.

- ***Aggregation, pseudonymization, anonymization, and deletion whenever possible:*** This should be done at the outset of the processing, or as soon as personal data is not necessary for the processing purpose. When applying pseudonymization, the controller should store identification keys separately. A partially overturned recent German court ruling indicates that such measures are merely indicative and that the controller's legitimate interests may outweigh DPbD&bD considerations.

Case DE-CR-3: Social media users do not have a right to use pseudonyms instead of their real names[108]

The Higher Regional Court of Munich ruled that a social media operator's requirement for users to use real names instead of pseudonyms on the platform did not violate Article 5(1)(c) of the GDPR. In its ruling, the court held that pseudonymization is only an indicative example of a TOM under Article 25(1) and is not a mandatory requirement for controllers, and individuals do not have a right to pseudonymization. The court saw the controller's identification policy as necessary for the platform's safety and accountability and as a proportionate measure since it outweighed the user's right to informational self-determination in the case. Moreover, the court held that the provision under the German Telemedia Act (TMG), which in principle obliged social media companies to allow its users to use their service under a pseudonym or in an anonymous fashion, should be interpreted in line with the GDPR to avoid any direct contradiction. In other words, where letting users use a pseudonym would not be reasonable for the controller to pursue its legitimate goals, the latter should not be forced to provide that option to its users.

The German Federal Court of Justice (Bundesgerichtshof) partially overturned the judgment, allowing the plaintiff to change his profile name to a pseudonym and use his preferred username to access the functions of his user account. The court conducted a balancing exercise by stating that companies should be free to determine the nature of their economic activity under Article 16 EUCFR and have a legitimate purpose when asking for a real name, while users have the right to the protection of personal data and the right to respect for private and family life (under Articles 8 and 7 EUCFR). Then the court noted that when weighing the conflicting fundamental rights, it is essential to differentiate between the internal relationship between the contracting parties and the user's ability to remain unrecognized by third parties. The latter is of particular importance given that the indication of a real name accompanied by the sharing of other information can render users' personal data widely available. Thus, and also because of the TMG provision that asks for a true indication of a name only in exceptional circumstances, the platform's real name policy in its terms and conditions is invalid and users should be able to use a pseudonym (**Case DE-CR-4**).[109]

iv. Accuracy

Early and ongoing compliance with the Article 5(1)(d) accuracy principle is crucial given that inaccurate data can lead to wrongful analysis and consideration of an individual's situation and generate material and non-material harm. The EDPB Guidelines list key design and default accuracy elements that are corroborated by several DPAs' corrective actions. These include:[110]

- ***An appropriate degree of accuracy according to reliable measurements:*** each personal data element should be as accurate as necessary for the specified purposes, and the controller should seek to reduce the number of false positives/negatives.

Case IE4: The submission of inaccurate data by third parties does not exempt the controller from responsibility[111]

In 2018, the Irish Credit Bureau (ICB) — which provides creditworthiness reports to borrowers and lenders — changed their code to improve the accuracy of their data. However, due to a technical fault, the change resulted in the inaccurate update of 15,120 loan records for a two-month period. When the ICB detected the error, it fixed it and informed those affected, as well as the Irish DPC. With regards to Article 25(1) and the data accuracy principle, the DPC determined that the controller must ensure that inaccurate data will not be stored in the database, and also the fact that the data was provided by ICB member financial institutions does not reduce the controller's obligation of ensuring that all information is accurate.[112] Moreover, given the inherently sensitive nature and the volumes and variety of data categories at stake, the risk of inaccurate personal data being processed in ICB's database is high and appropriate measures should be taken. For the DPC, such measures should have included those that were mature and readily-available solutions at the time of the data breach, such as a comprehensive documented change management process.

The DPC issued a reprimand for the violations of Articles 5(2), 24(1), and 25(1) GDPR, plus an administrative fine of 90,000 EUR for the breach of the latter provision.

- ***Source reliability, continued accuracy, and updated personal data:*** the sources of personal data should be reliable and the controller must verify the correctness of the personal data undergoing processing and correct or update them, if needed. This dimension of accuracy as it relates to DPbD&bD has been a particular area of focus for the Finnish DPA. Decisions in this regard may serve as a cautionary tale for businesses collecting data from publicly-available sources to train algorithms, including generative AI models.

Case FI8: Credit information company is responsible when it collects inaccurate information from third party sources[113]

Bisnode Finland Oy, a credit information company, was generating debtor creditworthiness reports based on information it extracted from court cases included in the "the Legal Register Centre," a public Finnish institution. In 2017, a Finnish court found that between 2011 and 2017, courts were often wrongly identifying debtors as unwilling or unable to pay. Therefore, the information generated by the Centre was not accurate.[114] The Finnish Data Protection Ombudsman determined that Bisnode's processing of information contained in the Legal Register Centre database breached Articles 25(1) and 5(1)(a) GDPR since it was not capable of detecting which cases it should consider in its creditworthiness assessments, resulting in incorrect reports. It is interesting to note that the DPA determined there was an infringement of the lawfulness principle and not the accuracy one, despite the fact that the shortcomings were related to the inaccurate nature of the personal data processed by the controller. This determination is different from the DPA's stance in **Case FI9**, in which the regulator found that the Legal Register Centre did not implement sufficient measures to ensure that only accurate data was stored and published in its database, according to Article 5(1)(d) GDPR. Continuous accuracy throughout the lifecycle of processing requires that tests are performed at critical stages, which the Centre failed to do. Moreover, the Centre failed to secure a lawful basis for divulging litigants' personal data according to Article 5(1)(a) GDPR. For the DPA, both were linked with a breach of Article 25(1) GDPR.[115]

- ***Use of technological and organizational design features to decrease inaccuracy:*** the importance of safeguarding the principle of accuracy through effective measures can be seen in an enforcement action from the UK DPA (the Information Commissioner's Office, or "ICO"), even if Article 25 was not explicitly mentioned. Nevertheless, the actions ordered by the ICO should be seen as merely indicative and mostly organizational measures that could enable compliance with Article 5(1)(d) GDPR.

Case UK1: Leaving a message to the wrong recipient reveals the systematic use of inaccurate data[116]

A staff member from a housing company called Starts With You (SWY) mistakenly left a message on the telephone number of a data subject's husband, instead of the data subject's own number. The message included the data subject's new address, which had been provided to SWY by its parent company, Bolton at Home (BH). Both the data subject and her allegedly abusive husband were already registered with BH, but the data subject applied for the new property in her name only. After becoming aware of the data breach, BH reported it to the ICO, albeit in a late fashion. The Commissioner found a violation of Article 5(1)(d) GDPR, as BH did not ensure the personal data processed was up-to-date by merely copying over the data subject's information from the previous record, rather than starting afresh. Therefore, the Commissioner ordered the company to implement an appropriate client record, formalize policies concerning warning codes for abuse, review internal breach reporting policies and processes, and provide adequate training to staff on data processing policies and processes.

v. Storage Limitation

Another key principle under Article 5 GDPR, storage limitation, has often been the focus of DPAs' enforcement actions that touched on DPbD&bD. Under the GDPR, controllers need to ensure, via appropriate TOMs, that they do not store personal data in a form that permits identification of data subjects for longer than is necessary for pursuing the processing purposes. This obligation includes establishing time limits for erasure or for a periodic review of such time limits, as well as establishing expiry dates for automated deletion or anonymization of personal data.[117] For the EDPB and a number of national DPAs that have applied the storage limitation principle in combination with Article 25(1) GDPR, key design and default storage limitation elements include:[118]

- ***The determination of the categories of data and the length of storage that is necessary for the processing purpose, paired with an appropriate justification.*** Furthermore, the controller should be able to disclose the rationale behind and legal grounds for the retention period. The phenomenon of not defining periodic personal data deletion policies generates the risk of creating what the Berlin DPA calls "data graveyards."

Case DE1: Data graveyards happen when no retention period exists[119]

The German State of Berlin DPA (BInBDI) issued an administrative fine of 14.5M EUR against Deutsche Wohnen SE, a Berlin-based real estate company, after an investigation initiated in June 2017 revealed that the company structurally failed to delete personal data of tenants stored in its archive. The company violated Articles 5(1)(a)(c)(e) and 25(1) of the GDPR by storing personal and financial information without a valid reason and not providing for data removal. In the associated press release, Berlin's Commissioner for Data Protection Maja Smoltczyk highlighted that this type of "data graveyards" is something that DPAs frequently encounter in supervisory practice. The BInBDI also fined Deutsche Wohnen SE in 15 individual cases for unauthorized storage of tenants' personal data, with fines ranging between 6,000 and 17,000 EUR.

- ***The adoption of procedures for data deletion and anonymization, including in an automated way when appropriate.*** Furthermore, the controller must test the effectiveness of its deletion or anonymization processes in an ongoing manner.

Case NO2: The importance of automating personal data deletion[120]

The Norwegian Datatilsynet found that the Norwegian Public Roads Administration kept data from "toll road crossing logs" — such as license plate numbers and location and times of crossing — for an inappropriate period of time (i.e., more than 10 years). For the DPA, this retention was due to a lack of appropriate measures that would ensure built-in protections such as an automated deletion functionality. The DPA ordered the Administration to delete all unnecessary personal data and revealed that they intended to issue a NOK 4,000,000 (approximately 360,000 EUR) administrative fine for violations of Articles 5(1), 17(1)(a), 17(1)(d), and 25(1) GDPR.

vi. Integrity and Confidentiality

Article 5(1)(f) and its explicit reference to TOMs as the way controllers are expected to ensure appropriate security of personal data lays out the significant overlap between DPbD&bD and the integrity and confidentiality principle. This overlap is also clearly supported by Recital 78 GDPR, which notes that TOMs in in this regard should meet the principles of DPbD&bD and gives examples of measures such as pseudonymizing personal data and continuously monitoring and improving security features. It is not by chance that the list of design and default elements that the EDPB wishes controllers to consider with regards to integrity and confidentiality is the longest in its DPbD&bD guidelines.[121] We also note that simultaneous breaches of the integrity and confidentiality principle and Article 25(1) GDPR are often associated with breaches of the GDPR's provision on data security (Article 32), although that is not always the case.

Below we explore which among these above elements were the most explored in DPAs' corrective actions since May 2018. It is noteworthy that a large chunk of these actions came from organizations reporting significant data breaches or DPAs being informed of breaches or issues through other means (i.e., media stories, data subject complaints), rather than DPA ex officio actions. For DPAs, the occurrence of multiple data breaches offers a strong indicator of a breach of the integrity and confidentiality principle, coupled with Article 25(1) GDR infringements.

Case RO2: Processing loan requests with inaccurate personal data breaches confidentiality principle[122]

The Romanian ANSPDCP received 17 notifications concerning data breaches suffered by Raiffeisen Bank SA. In its investigation, the DPA found, among other facts, that the bank was notifying customers that their request for a loan was approved even though the customers had never made such requests nor did they sign any related documents, all the while using incorrect contact information and therefore sharing personal data with the wrong recipients. The DPA, determined that the bank did not take measures to ensure that it processes personal data only at the request of its customers, nor did the bank implement adequate TOMs to ensure appropriate protections against the risks of unauthorized access to and/or disclosure of personal data. The DPA established a breach of Articles 5(1)(f) and 25(1) GDPR, and issued three warnings and a 28,000 EUR fine against the bank (5,000 EUR of which were for infringements of DPbD&bD).

The DPAs seem to generally follow the EDPB Guidelines in detecting whether Article 25(1) has been violated in tandem with an infringement of the principle of integrity and confidentiality, by considering elements such as:

- ***Access control management,*** concerning both the number of people that access the data and the content that is being accessed. This element means limiting access on a need-to-know basis, such as limiting access to only data categories that are needed to perform the processing operation that has been assigned to the specific person.

From our research, one DPA decision and one court ruling stand out as representative examples of the issues that come from a lack of access control management tools:

- **Case DK1 on lack of monitoring of unauthorized access.**[123] The Kolding Municipality processed documents containing personal data in around 400,000 cases without taking appropriate TOMs. The tool that the municipality had been using for managing system access permissions for several years was unilaterally changed by the municipality's supplier. This change meant that all documents became directly available to the municipality's 2,400 employees, which the controller failed to detect for several years. The Danish DPA (Datatilsynet) noted that a lack of periodic access management control through audits creates a high risk of inadequate or deficient security measures not being identified in a timely manner. Although the decision did not mention Article 25 GDPR, the DPA found a violation of Article 32(1) GDPR because of the failure to continuously monitor inappropriate access permissions.
- **Case FR-CR-1 on access to health records for auditing purposes:**[124] The National Council of Physicians sought to annul a French law that authorized auditors and external service providers to access patients' data.[125] The Conseil d'Etat ruled that due to insufficient TOMs, such access in healthcare systems and facilities was not limited to data only strictly necessary for the completion of the prescribed tasks (such as the control of invoicing) and annulled the challenged law. More specifically, with regard to the access given to auditors, the Conseil d'Etat determined that a certain degree of access to health data was necessary to calculate and verify revenues, and that the law prescribed measures such as limiting access to data to when it is necessary in that context. Nevertheless, the Conseil d'Etat ruled that *the law should have incorporated more robust measures such as the pseudonymization of data in order to ensure that data subjects' right of medical confidentiality is safeguarded in line with Articles 6 and 25 of the GDPR*.

- ***Protection according to risk:*** All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separate from the rest of the personal data. In many cases, DPAs acknowledge that when sensitive data is being processed, enhanced safeguards should be in place. As the below decision from the Belgian DPA shows, it is not necessary for risks of data breaches from insufficient security measures to materialize for the DPA to initiate a corrective action.

Case BE5: Access to medical results via an insecure website[126]

A laboratory's website allowed doctors to access their patients' test results and medical records in real time. However, the website used the unsecured "http" protocol instead of the "https" one and was vulnerable to cyberattacks. Upon a complaint from one of its clients, the laboratory updated its security measures and argued that no attack had been detected in the past. After an investigation by the Belgian DPA's Inspection Service triggered by a complaint from the data subject, the Litigation Chamber decided that at the time of the complaint there were no appropriate security measures in place and a lack of cryptography in the web platform violated the principles of integrity and confidentiality under Article 5(1)(f) GDPR and DPbD&bD. The DPA decided to issue a fine of 20,000 EUR.

Case IS2: Former employees should not be able to access sensitive personal data[127]

Due to a lack of TOMs, S.Á.Á. medical institutions (S.Á.Á.) did not prevent a former employee from accessing medical records in paper form. The records concerned 252 individuals and included therapists' notes from interviews with patients and other accompanying documents. For the Icelandic Persónuvernd, the fact that the employee was able to transfer these documents from the institution to his own premises meant that no appropriate measures were implemented to prevent such actions. The DPA also noted that given that the purpose of the processing was to provide healthcare to people with alcohol and drug addictions, the controller should have implemented higher safeguards to ensure that the data were stored securely. The regulator imposed a fine of 3,000,000 ISK (approximately 20,000 EUR).

- ***Secure transfers:*** data transfers should be secured against unauthorized and accidental access and changes. In this respect, DPAs are more likely to find breaches of the integrity and confidentiality principle under Article 5(1)(f) GDPR in combination with DPbD&bD in cases of systematic unsecure transfers of personal data or, in cases of one-off sharing of data with unauthorized third parties, when particularly sensitive data is at stake. Even if DPAs are more prone to issue mere reprimands in cases of isolated incidents (see **Cases PL7** and **PL11**[128]), these situations with isolated disclosure of personal data can reveal structural failings of controllers to implement adequate TOMs and indicate unwarranted disclosure can be happening on an ongoing basis.

In some cases, DPAs and courts found breaches of Article 25(1) GDPR where there was a one-off disclosure of sensitive personal data to unauthorized recipients:

- **Case IS3 on sharing student data with unauthorized supervisors and guardians**[129]: A teacher erroneously attached a file to an email that contained sensitive personal data concerning 18 students. The information concerned the students' well-being, academic performance, and social conditions, including about their mental and physical health. After receiving a data breach notification from the school and following an investigation, the Icelandic Persónuvernd found that the school lacked robust TOMs that would have prevented such data sharing and imposed a fine of ISK 1,300,000 (roughly 8,600 EUR) for a breach of Article 25 GDPR.
- **Case BG-CR-1 on parcel delivery to the wrong recipient**[130]: The Bulgarian Administrative Court upheld the roughly 500 EUR fine imposed by the Bulgarian DPA (CPDP) against the courier company Speedy AD for unlawfully disclosing personal data to a third party by delivering a parcel to a person other than the intended recipient. In this case, despite a timely telephone call to the controller from the addressee alerting to the fact that he did not live at the given address, the parcel was nevertheless delivered to another person and signed by them. This practice was in line with what the controller argued were the "usual rules of the industry." The Bulgarian Administrative Court determined that the company violated Articles 5(1)(a), 5(1)(f), 24, and 25 of the GDPR because it failed to verify the identity of the recipient; the instruction given to the courier to identify the recipient natural person only by requesting the first and last name did not ensure the delivery of the parcel to the correct recipient.

- ***Secure storage:*** Data storage shall be secured from unauthorized access and changes. This obligation means that the controller should, inter alia, determine whether specific types of data merit enhanced protective TOMs, as well as opt for centralized or decentralized storage, depending on the level of risks.

Case FI10: Clients' data made publicly available through insecure storage[131]

In this case, a Finnish travel agency used an unencrypted network connection in its visa application form and stored personal data in an open server. The Finnish Data Protection Ombudsman noted that the controller could not prove that it had implemented other measures — such as restriction of traffic or access controls — and thus details contained in the visa application form could be accessed by third parties without sufficient restrictions. This determination means that the agency violated Articles 25(1) and 32 GDPR, along with the principle of integrity and confidentiality under Article 5(1)(f) GDPR. In December 2021, the sanctioning board of the DPA imposed a fee of 6,500 EUR on the agency's parent company.

Case BE6: Unique identifiers for behavioral advertising purposes should be protected against modification[132]

The Belgian DPA found that the Transparency and Consent Framework (TCF), developed by IAB Europe, failed to comply with a number of provisions of the GDPR. The TCF is a widely used mechanism for managing user preferences for online personalized advertising, and plays a pivotal role in Real Time Bidding (RTB).[133] With regards to the principles of integrity, accountability, and DPbD&bD, the DPA noted that the controller did not put forward TOMs to ensure the integrity of the TC String — which stored users' choices with regards to the processing of their personal data for behavioral advertising purposes — as prescribed by Articles 5(1)(f), 25, and 32 GDPR. For the latter, the IAB should have guaranteed the integrity of the TC string by safeguarding it against a possible falsification or modification. The DPA imposed an administrative fine of 250,000 EUR.

- ***Implementation of an information security management system, early risk analysis, security by design, and regular review of all systems to detect vulnerabilities.*** This obligation includes measures establishing policies to prevent employees from using personal devices and email addresses for business purposes, or regularly testing IT systems for risks of unauthorized access and attacks.

Case IS4: Usage of personal means for business purposes[134]

The Icelandic Persónuvernd found a violation of Articles 25 and 5(1)(f) GDPR regarding an employee of Hafnarfjörður's child protection committee who used his personal smartphone to take notes that he later used to draft work reports. This violation was despite the fact that the employee usually sent the notes to his professional email address and deleted them from the phone afterwards. While the DPA did not impose a fine, it still ordered the committee to prohibit employees from processing personal data by using their personal equipment — such as phones and computers — and personal email addresses.

Case PL8: Failure to continually assess security measures in IT systems[135]

Virgin Mobile Polska, a telecommunications provider, detected that unauthorized third parties gained access to the personal data of 114,963 of its customers and reported such data breach to the Polish UODO. Such unauthorized access was made possible because of a vulnerability of the IT system, as the company did not verify how secure the process of generating a confirmation of a prepaid card registration was. For the DPA, the company failed to safeguard the principle of confidentiality, given the system's weak verification mechanism. The controller's measures should have included regular testing and evaluation of the adopted security measures according to a specific and documented timetable. The controller's omissions resulted in a violation of Article 25(1) GDPR, as the DPA noted that the obligations under the provision apply both to the design and data processing stages. For the DPA, data "security implementation is an ongoing process, not just a one-time action by an administrator." The regulator issued a fine of PLN 1,968,524 (equivalent to 460,000 EUR).

vii. Accountability

According to the EDPB Guidelines, the accountability principle is overarching, as it requires the controller to be responsible for choosing the necessary TOMs to ensure and demonstrate compliance with the remaining Article 5 GDPR principles at all times.[136] An important decision from the Italian DPA in this regard mentions Recital 74 GDPR when noting that Articles 5(2), 24, and 25 GDPR place a general responsibility on the controller of demonstrating that any processing carried out either directly by the controller or via its processors has been done in compliance with the data protection principles.

Case IT7: Energy company did not implement measures to prevent and tackle instances of unsolicited promotional calls operated by unauthorized third parties[137]

The Italian Garante initiated an investigation into Enel Energia after receiving multiple complaints from individuals about unwanted promotional calls. In its defense, the controller argued that it has been a victim of "scammers" working for competing companies, as the latter were using the name of Enel Energia to promote their own products and services. The Garante noted that this could not exclude the company's liability since it did not provide enough evidence regarding the actions of its competitors. For the Garante, it is crucial that the controller implements effective and adequate measures on a case-by-case basis through structured and systematic verification mechanisms. By doing so, data protection obligations are not reduced to a purely paper-based exercise and accountability is preserved. In the present case, the DPA stated that incidents of unwanted calls should have been an "alarm bell" for the controller, who is a "leader in the Italian energy market and always a protagonist of the economic-productive life of the country." In that sense, the Garante determined that the company should have tackled the problem "at its root" by not focusing only on GDPR compliance of its "official" sales network. The Garante issued multiple corrective measures and a fine of over 26.5M EUR.

Another decision from the Spanish DPA highlights how controllers who wish to comply with the accountability principle and Article 25 not only need to keep a close eye on their own external representatives, but also on persons that deem to represent their customers. It is particularly important for companies to check whether such persons have a valid and broad enough mandate to represent the data subjects in their contractual relationship.

Case ES3: Energy company exercising insufficient verification of its customer representatives' powers[138]

Another energy company, EDP ENERGÍA, S.A.U, allowed a customer's representative to carry out certain actions, such as transferring data to third parties or signing binding contracts, without exercising sufficient control over these actions and without determining whether the representative had the power to pursue them. According to the Spanish AEPD, the controller did not identify all possible risks that this lack of control entailed and did not implement a system that would control and ascertain the exact representation powers of the representatives. Thus, in instances where the representatives lacked appropriate powers, the controller could be lacking an appropriate lawful ground under Article 6 GDPR to process their customers' personal data. Thus, by not exercising sufficient control over the representatives, the controller did not abide by its accountability obligations and also breached Articles 5(1)(a) and 25 GDPR. The DPA issued a fine of 1,500,000 EUR, of which 500,000 EUR were due to a violation of Article 25 GDPR.

b. DPAs focus on data subjects' rights and freedoms enshrined in the GDPR

DPAs tend to mention, quite abstractly, that a controller is in violation of Article 25 GDPR due to a lack of safeguards for data subjects' rights and freedoms. It is clear that the reference to rights and freedoms is not intended to be restricted to data subjects' rights under Articles 12 through 22 GDPR, but also encompasses fundamental rights and freedoms other than the protection of personal data under Article 8 of the Charter. Nevertheless, DPAs tend to focus on GDPR rights in the few cases where they assessed controllers' compliance with this dimension of Article 25. Where they did so, DPAs identified what specific right was infringed by the measures implemented or omitted by the controller.

For instance, an infringement of the right to erasure under Article 17 GDPR can trigger a violation of Article 25(1) GDPR. But the right to erasure, like all other rights under the GDPR, is not absolute, and can be limited by the right of the controller to conduct its business.

Case AT1: Partial deletion of personal data in loyalty programs is not possible[139]

In this case, the controller was a retail business that ran a customer loyalty program. In order to participate in the program, a customer had to register for a loyalty card and agree to the data protection statement. The complainant accepted the statement but later on asked the company to delete part of his personal data, such as data concerning shopping time and place. The company refused to abide by the client's request and instead offered to delete all of his personal data. After the client complained to the Austrian DPA (DSB), the regulator held that a data subject should be free to request the deletion of only part of their data. This is because the controller is bound by the accountability principle (Article 5(2) GDPR) and the related obligations under Articles 24 and 25 GDPR, and thus must satisfy data subjects' rights to the extent requested by the individual, even if only partially, unless the controller can justify why this cannot be done (e.g., because it is not technically possible). However, for the DSB, the decision of the controller to not adopt measures to enable it to only partially delete data did not breach the GDPR; the right to erasure should be balanced against the right of the company to operate its loyalty program, which would be precluded if it were obliged to satisfy partial deletion requests from individuals that participated in the program.

Beyond **Cases IE3** and **ES1,** which we previously explored, other DPAs also determined that a violation of Article 15 GDPR on the right of access can mean a violation of Article 25(1) as well, notably if a system is not designed to enable the extraction of personal data to be shared with data subjects.

Case HU2: Access to video recordings[140]

A customer of the Deichmann company requested access to footage captured by one of the controller's stores' CCTV cameras, which the controller refused. Pursuant to a complaint it received from the customer, the Hungarian NAIH noted that the controller was breaching the complainant's right of access. Moreover, with regards to Article 25(1) GDPR, the controller ought to have already implemented appropriate measures from the design phase of its processing activities (i.e., before installing cameras in the store) that could guarantee the right of access under Articles 15(1) and 15(3) GDPR. The DPA explained that indicative organizational measures included: setting internal procedures for handling data subjects' requests; creating and informing data subjects about appropriate channels and conditions for exercising their GDPR rights; keeping a record of processing activities under Article 30 GDPR; and training employees on data subject request-handling. The DPA issued a fine of 20,000,000 HUF (roughly 50,000 EUR).

Not providing data subjects with transparent information may also lead to the violation of the DPbD&bD principle. In a landmark decision from the Hungarian DPA on the use of an AI system to optimize customer support by arguably detecting customers' emotions, breaches of the right to information were linked to other infringements of the GDPR related to lawfulness, purpose limitation, and accountability. As EU lawmakers discuss whether this type of system should be prohibited or included in the list of high-risk use cases under the upcoming rules on AI, the Hungarian DPA's enforcement action shows how challenging GDPR compliance can be for controllers deploying such systems.

Case HU3: Detecting and measuring customers' emotions needs appropriate transparency[141]

In a decision issued in February 2022, the Hungarian NAIH sanctioned Budapest Bank for unlawfully processing voice recordings through an automated system that promised to detect and measure the emotions of customers who called the bank's helpline. The system prioritized returning the calls of customers who "sounded" the most upset and impatient. The DPA found multiple breaches of the GDPR, including the principles of lawfulness, transparency, and purpose limitation; notice obligations; the right to object; controller accountability obligations; and DPbD&bD. Concerning the latter, the DPA determined that the controller breached Article 25(1) and (2) GDPR because it failed to appropriately balance the interests of the company with the data subjects' rights and freedoms — notably, their right to information — as the controller did not inform them about the use of sound analysis software. The DPA noted that especially when the technology used is complex, the information granted to data subjects should be given in a comprehensible way. In essence, the bank, by using the automated voice analysis system in its operations, violated Article 25 for not considering the high risks for data subjects and for not granting them transparent information. The DPA issued a fine of 250,000,000 HUF (approximately 700,000 EUR) and an order to bring the processing into compliance.

2.3. Data Protection by Default should prevent the manipulation of individuals online

The controller has to implement appropriate TOMs, both at the time of the determination of the means for processing and at the time of the processing itself, in order to ensure that, *by default*, only personal data that is necessary for each specific purpose of the processing is processed and personal data is not made accessible without the individual's intervention to an indefinite number of natural persons. The EDPB Guidelines define "default" as referring "to the preexisting or pre selected value of a configurable setting that is assigned to a software application, computer program or device."[142] Thus, for the purposes of Article 25 GDPR, data protection by default refers to such choices made by the controller.[143] This definition is particularly important when it comes to assessing the lawfulness of specific configuration of online interfaces and tools used by data subjects, and the proliferation of deceptive design patterns.

The controller has to ensure that, by default, only personal data that is necessary for each specific purpose of processing is being processed. In other words, the TOMs should aim at safeguarding the data minimization principle[144].

Case FI11: Collection of location data should not occur as a default[145]

Also in Finland, and following a data breach notification, the Data Protection Ombudsman found that the Northern Savonia Hospital District had breached Articles 5(1)(c) and 25(2) GDPR because the hospital's employees' professional portable devices had their location setting automatically enabled. According to the DPA, the processing of location data was unnecessary and unlawful because the controller should have processed only as little personal data as necessary to manage the relationship with its employees. Furthermore, the DPA ordered the hospital to delete any historical data, location logs, and other personal data generated when using the location data feature.

However, the wording of Article 5 and Article 25(2) of the GDPR establish that data protection by default entails not only that controllers collect (by default) personal data that is adequate, relevant, and limited to what is necessary, but also that the data is collected for specified, explicit, and legitimate purposes (i.e., in line with the purpose limitation principle). Moreover, through the lens of DPA decisions, Data Protection by Default seems equally relevant for the principles of storage limitation and confidentiality.

Case IS5: Processing student data for direct marketing breaches purpose limitation[146]

The Icelandic Persónuvernd investigated the student management information system "Seesaw" used by the City of Reykjavík. With regards to Article 25(2) GDPR, the DPA concluded that the City of Reykjavík did not implement the appropriate measures in order to ensure the principles of purpose limitation, data minimization, and storage limitation. For the DPA, since the processing of personal data for direct marketing did not fit into the processing purposes set by the City of Reykjavík, asking parents and guardians to opt-out was not enough; on the contrary, the default setting should have avoided processing for such a purpose. On the other hand, student folders should have been accessible only to teachers, parents, and guardians. The DPA suggested that the City of Reykjavík close the Seesaw accounts of school children and ensure that all their personal data is deleted from the system, after extracting a copy of such personal data for physical record-keeping.

Under Article 25(2), the measures safeguarding data protection principles should concern: *the amount of personal data collected*, meaning that when less granular data is sufficient any surplus personal data shall not be collected; *the extent of the processing of the personal data and its storage period*, meaning that data should as a default be deleted or anonymized; and *the accessibility of personal data.*[147]

Concerning the latter aspect, Article 25(2) GDPR states that personal data should not be made accessible without the individual's intervention to an indefinite number of natural persons. The EDPB Guidelines note that "the opportunity to intervene could either mean to ask for consent to make the personal data publicly accessible, or to provide information about the public accessibility in order to enable data subjects to exercise their rights in Articles 15 to 22."[148] The following cases emphasize the importance of controlling the default settings in terms of what data is made accessible and to whom. The matter has also been examined by the CJEU, albeit on a superficial basis.

Case IE2: Social media user searching tools made personal data accessible to an unlimited number of people[149]

In the case that we started analyzing in Section 2.1.e. above, the Irish DPC found two distinct issues regarding the incompatibility of Facebook's user search tools with Article 25(2) GDPR, notably:

a. Searchability settings for users regarding certain features were set to include phone numbers and email addresses by default, and users had to manually change this setting.

b. When a user added their phone number for two-factor authentication (2FA), the number was automatically and by default made searchable in Facebook's tool. Thus, users had to change their settings to prevent this. Also, adding a number for 2FA meant that the number could be used to "find friends" and no option existed to exclude this function.

The DPC determined that Meta Platforms Ireland Limited (Meta), by including users' phone numbers and email addresses by default in its user search tools, made this personal data accessible to an indefinite number of people without the users' intervention. This in turn made the available data vulnerable to scraping practices and rendered users' profiles searchable even if they had not submitted their phone numbers for searchability purposes. Therefore, Meta violated Article 25(2) GDPR, for which it was ordered to pay an administrative fine of 115M EUR.

Case FI12: Publicly-available data should still not be disseminated[150]

A Finnish company offering parking facilities requested car owners to use a parking permit tag with their home address and specific parking space. In the complaint-triggered proceedings before the Finnish Data Protection Ombudsman, the controller argued that car owners' addresses were publicly available information in any case, as other persons could find such addresses by consulting the Land Registry with the car's license plate number. However, the DPA noted that the controller failed to show how such information was necessary for controlling illegal parking and that the address could be replaced with other unique identifiers. The DPA also pointed out that *regardless of whether some information is publicly available, the controller should still comply with Article 5(1)(c) GDPR and 25(2) GDPR by ensuring that by default only the personal data necessary for the specific purpose of the processing is processed, and by not making data available to an unlimited number of people*.

Case CJEU1: Beneficial ownership register should be accessible only on request[151]

In this case before the Luxembourg District Court before the CJEU, company Sovim requested the Luxembourg Business Registers (LBR) to restrict access to information about its beneficial owners only to certain entities instead of being publicly available. The open-data system of the Register allowed anyone to access beneficial owners' personal data, including sector-specific investments. The national court requested the CJEU for a preliminary ruling asking for, inter alia, clarifications on Article 25(2) GDPR, which states that personal data shall not be made accessible without the individual's intervention to an indefinite number of natural persons. The court asked whether it is in accordance with Article 25(2) GDPR to grant access to the Register without demanding the creation of an account and without restricting the extent and accessibility of the personal data that can be consulted. The CJEU determined that public access to beneficial ownership information under the amended Anti-Money Laundering Directive interferes with the fundamental right to privacy and personal data protection and the interference is justified but not limited to what is necessary for the objective pursued. Thus, it is not proportionate to the aimed goal, and access to the Register should be granted only on the basis of justified requests from natural or legal persons The CJEU reached this conclusion without elaborating specifically on the question concerning Article 25(2) GDPR.

Beyond cases of pre-ticked consent boxes like **Case BE2**, default settings such as web design choices were deemed as an intrusion on individuals' privacy or a violation of other rights they possess. It is noteworthy highlighting the overlap between enforcement actions in this space and the recently-approved EDPB guidelines on deceptive design patterns in social media platform interfaces. The guidelines state that Article 25 GDPR plays a vital role in deceptive design pattern assessments, as applying appropriate TOMs before launching an interface design helps providers avoid deceptive design patterns in the first place. The practices, which were sanctioned by the French DPA in the Discord case, could be seen as examples of "deceptive snugess" or "misleading action" as defined and illustrated in such guidelines.[152]

Case FR1: Users click on the "X" icon on the main window of an app and still remain connected to the chat room[153]

Discord is a voice and instant messaging software that allows users to communicate via microphone, webcam, and text, as well as create servers and it is available on various platforms, such as Windows, Mac, Linux, iOS, and Android, but can also be accessed through a web browser. The service is free but users can subscribe for additional features. Discord explained that, as a default, when users clicked on the "X" icon on the main window of the service, they were not actually leaving the application; they were still connected to the chat room. For Discord, this default setting was intentional since the primary function of the application was to allow users to chat with their peers while navigating in other applications or while browsing the web and, since similar applications operate in the same way, users of Discord would reasonably expect such operation. Finally, Discord noted that the users were able to change the setting and be able to disconnect from the application by just clicking on the "X" icon. For the French DPA (CNIL), the user could not reasonably expect that clicking on the "X" button signified the minimization of the application given that other communication applications, when users are about to quit the application, inform them with a pop-up window or give them the option to manually put the application in the background. The default configuration of the application could lead to third parties accessing users' personal data. As CNIL noted, "the user was not necessarily aware that his words continued to be transmitted and heard by the other members present in the vocal room [...] such a configuration, in the absence of sufficiently clear and visible information, presented significant risks for users, in particular intrusion into their privacy." Therefore, the CNIL found that Discord violated Article 25(2) GDPR and imposed a fine of 800,000 EUR.

2.4. Divergent practice emerges related to non-material damages for DPbD&bD breaches

One of the key enforcement measures of the GDPR, including of Article 25, is judicial redress, which also encompasses the right of individuals to obtain compensation for non-material damages. Academics have claimed that "since Article 25 GDPR primarily imposes an organizational obligation on the controller, violations against it should not in themselves lead to claims for damages by data subjects under Article 82 GDPR and such claims should only arise as a result of unlawful processing or the lack of granting of data subjects' rights".[154] During our research, we have found divergent practice on this question, particularly stemming from German courts.

Case DE-CR-1: Article 82 GDPR limits compensation claims to processing-related damages[155]

This case involved an unnamed social media platform that offered users the ability to create personal profiles and share personal information with others. Initially, the platform's default settings allowed anyone to find a user's profile on the platform by entering their email address or mobile number, if the user had provided them. These settings resulted in data scraping incidents, and in April 2021, data from approximately 553 million users in 106 countries was published online. The plaintiff claimed to be among the users' whose data was scraped and requested compensation for non-material damages. Specifically, the plaintiff claimed to have experienced a considerable loss of control over their data and remained in a state of great unease and concern about possible misuse of their data.

However, ***the Regional Court of Heilbronn ruled that the plaintiff was not entitled to compensation under Article 82(1) of the GDPR, as no subjective right can be derived from Article 25.*** The court determined that, according to Recital 146 of the GDPR, even though the concept of damage must be interpreted broadly, the basic prerequisite for non-material damage is that it must be "suffered," (i.e., actually incurred and not merely feared, causing a "noticeable impairment" of the injured party). The court concluded that the plaintiff's "state of discomfort" and the receipt of emails were not sufficient to constitute non-material damage.

On the other hand, another January 2023 German court ruling about the exact same issue seems to open the door to compensation claims based on a breach of Article 25 GDPR, as long as the plaintiff is able to demonstrate the infringement led to damages. As these court cases relate to making social media data vulnerable to data scraping, we highlight that the Irish DPA has assessed such scenarios in a more holistic fashion under Article 25, namely in **Cases IE1** and **IE2,** analyzed later in this Report.

Case DE-CR-2: Lack of measures against data scraping entitles users to compensation[156]

In this case, the Stuttgart Regional Court was called upon to rule on the lawfulness of a default setting used by Facebook, which provided that all persons who have a user's email address or telephone number could find the user's profile if the latter had provided these contact details. Even though users could change the searchability setting, the plaintiff kept the default one active, which exposed his data to data scrappers. According to Facebook, it was "fundamentally impossible to completely prevent scraping of publicly viewable data without undermining the purpose of the platform," namely connecting users. The plaintiff asked, amongst other things, for compensation for non-material damages — loss of control over personal data and a sense of unease and concern about possible misuses of his data — as a result of a breach of Article 25(2) GDPR. The Court noted that the standard configuration of privacy settings must ensure that users make their data available only to the groups of people and only to the extent that they have defined themselves in advance. Also, pursuant to Article 82(1) of the GDPR, the controller is liable for damages due to breaches of the GDPR, irrespectively of the nature of the violated provision. Thus, a breach of Article 25(2) GDPR can give rise to a claim for compensation. Thus, the Court decided to order the defendant to pay the plaintiff a 300 EUR compensation plus interest.

The divergences between courts in and beyond Germany about the concept of non-material damage for the purpose of Article 82 GDPR may soon be settled by the CJEU in a line of pending cases on the matter.[157] The Advocate General's Opinion in the first of those cases suggests a narrow reading of the concept, leaving it up to national laws and judges to determine how it will be applied in specific cases, with the clear risk of fragmentation across the EU on the application of Article 82 in civil liability cases.[158] According to a more recent Opinion[159] in a case concerning a cyber attack at Bulgaria's tax agency, the AG noted that *"the fact that the data subject fears possible future misuse of his personal data could constitute, in itself, (non-material) damage giving rise to a right to compensation."* However, this detriment should cause actual and certain emotional damage and not simply trouble and inconvenience. This does not mean that there is a predetermined threshold of severity; "what matters is that it is not a purely subjective perception, changing and dependent on personality characteristics, but an objective harassment, even slight but able to be proven, in the physical or mental sphere or in the social relations of the person concerned".

3. SPECIFIC SCENARIOS RELATED TO NEW TECHNOLOGIES: DIRECT MARKETING, PETS IN ONLINE ENVIRONMENTS, AND EDTECH

In this section we will be analyzing three specific scenarios in which Article 25 GDPR was applied on multiple occasions, namely Direct Marketing, Privacy Preservation in Online Environments (and PETs), and EdTech. We chose to highlight case-law in these three scenarios given the high number of cases that we found and the fact that they reveal the impact of new technologies in the application of the GDPR. For the latter point, it should be noted that the advancement of technology not only challenges the way that GDPR rights are being applied but it also provides more options for a privacy-friendly mode of operation.

3.1. Direct Marketing: lack of consent and the right to object as a DPbD&bD infringement

Just like in **Case IT7** that we analyzed above, DPAs have extensively enforced Article 25 GDPR in regards to unsolicited communications for promotional purposes, with various references to the principles laid out in Article 5 GDPR. Additionally, regulators leverage the specific rules that apply to direct marketing under the GDPR — such as the absolute right to object to data processing for such purposes under Article 21 — in their corrective actions with PDbD&bD elements.
In certain cases, like Case **IS5** concerning the use of student data, DPAs found that Article 25 was violated in instances of direct marketing communications due to an infringement of the data minimization principle.

Case GR1: Mismatch between telco CRM and advertisers portal led to unwanted promotional calls[160]

A Greek telecommunications provider (OTE) was using two separate systems to keep track of its subscribers, the "CRM Siebel'' and the "portal"; an update to CMR Siebel concerning subscribers' data would trigger an instant update to the portal. Third-party advertisers had access to the portal in order to contact subscribers for advertisement purposes but due to a malfunction in OTE's overall system, the portal was not updated as it should have been, which resulted in more than 16,000 subscribers getting unwanted advertisement calls for more than three years. The Hellenic DPA (HDPA) determined that OTE should have incorporated appropriate and sufficient measures to ensure the accuracy of the data in its systems by carrying out accuracy checks. Since no such measures had been taken, the DPA ruled that there was a breach of Articles 25 and 5(1)(c) GDPR and imposed a 200,000 EUR fine.

DPAs have also used the lawfulness principle as a basis for determining a violation of Article 25 GDPR. The issue of lawfulness is of particular importance in the direct marketing context, as the ePrivacy Directive contains specific rules that apply to the sending of promotional messages through electronic means.[161] Such messages can only be sent with the individual's prior consent or on the basis of legitimate interests where the individual — who must be an existing customer of the controller — is given the chance to object at the start of the processing and within the context of every message.[162] Additionally, the CJEU has broadly interpreted the concept of "direct marketing" to also include "inbox advertising" (i.e., the display in the electronic inbox of advertising messages in a form similar to that of a real email).[163]

Case IT8: Promotional messages sent via Linkedin need a suitable legal basis[164]

The Italian Garante initiated an investigation after a complainant noted she had received an unsolicited Linkedin message from real estate company La Prima. In the message, the company proposed real estate services for one of the complainant's properties. For the Garante, the controller "used the real estate registry and the social network — set up for specific purposes — to propose a sales service, a different and incompatible purpose with the original ones." Furthermore, the regulator observed that such action was reasonably expected by the data subject, which meant that there was no valid legal basis under Article 6(1) GDPR. Furthermore, the Garante found a violation of Articles 24 and 25 of the GDPR and ordered the controller to adopt suitable TOMs to avoid carrying out promotional activities without a suitable legal basis.

In a number of other decisions related to direct marketing practices, regulators have found breaches of Article 25 GDPR in connection with other key principles under Article 5 GDPR, including:

- **Accuracy (Case HU4)[165]:** The Hungarian NAIH fined Magyar Telekom, a telecommunications company, for sending unsolicited emails to an individual who repeatedly asked to have his email address deleted. The company asked the person to unsubscribe from promotional communications via their website, but the individual could not do so because he was not a customer. The DPA found that the company recorded contact details in a way that did not enable it to respond to data subjects' requests, which was a violation of Articles 5(1)(d) and 25(2) GDPR, resulting in a fine of 10,000,000 HUF (approximately 28,000 EUR).
- **Storage Limitation (Case BE7)[166]:** The case involved a company that was distributing "pink boxes" to pregnant women via partners and sharing their personal data for marketing purposes without informing them. When a customer started receiving promotional messages from other companies, she tried to withdraw her consent but kept receiving messages with offers. The Belgian DPA's Litigation Chamber identified violations of Articles 25(1) and 5(1)(c) GDPR, as the company failed to distinctly treat different processing purposes, did not communicate the individual's direct marketing objections to its partners, and had an excessive retention period of 18 years.
- **Accountability (Case IT9)[167]:** The Italian Garante found that telecommunications company Wind Tre breached Article 25 GDPR with regards to the methods of collecting, withdrawing consent, and opposing to processing for promotional purposes; to the control of its processors; and to the principle of accountability. Reasons for the violation pointed out by the Garante include that the company did not make withdrawing consent for data subjects as easy as giving it and did not monitor nor address instances of unsolicited marketing messages from its processors. The latter was related to the fact that the company's TOMs did not prevent misconduct from its processors, nor ensure that the data they inserted into the company's database and used for marketing messages had been acquired legitimately. These issues led to the Garante issuing several corrective measures, including imposing stricter controls of its processors and subprocessors practices, and the payment of a 16,729,600 EUR administrative fine.

A large number of cases revolved around the controller not respecting data subjects' right to object to the processing of their personal data for direct marketing purposes. Since this right under Article 21(2) GDPR knows no possible exceptions, unlike other types of processing that may rely on the legitimate interests lawful ground, these enforcement actions show the importance of controllers having processes, procedures, and systems in place to ensure they effectively halt data processing for direct marketing in case of an individual request to that effect. This includes instances where marketing messages are tailored on the basis of profiling.

Case GR2: Consequences of not acting upon data subjects' objection requests:[168]

A customer of the commercial company MZN kept receiving promotional messages even after exercising his right to object multiple times. For the Greek HDPA, even if the customer's first complaint was caused by an employee's mistake, the fact that he kept receiving messages was an indicator that MZN lacked necessary measures to ensure that data subjects' right to object was respected in line with Article 25(1) GDPR. The HDPA thus decided to impose a 20,000 EUR fine. Conversely, in **Case GR3**, where data subjects were not able to unsubscribe from KARIERA A.E.'s mailing list and kept receiving promotional messages, HPDA imposed a 5,000 EUR fine. The HDPA determined in this case that there was a breach of Articles 17, 21(2), and 25(1) GDPR. The HDPA noted that the technical issue that prevented objection and subsequent data deletion persisted for six months and affected 79 data subjects.[169]

The Italian DPA in particular has identified several instances where unwanted promotional calls came as a result of dysfunctional data management systems, which prevented systematic compliance with core GDPR principles and obligations.

Case IT10: The importance of mastering the management of contact lists[170]

Vodafone Italy S.p.A was accused of constant unwanted promotional communications and insecure storage of client data. The latter claim was based on the fact that non-authorized operators would frequently approach Vodafone's customers to incentivize them to subscribe to a different service provider or to request their ID credentials for fraudulent purposes. Vodafone argued it was applying 2FA to combat such incidents. The Garante highlighted that Vodafone's measures were not capable of combating the "undergrowth of telemarketing" since its management structure lacked a direct and functional connection between systems that organize promotional campaigns and systems that acquire the data of new customers. For the Garante, such system configuration is necessary to block access that is not attributable to promotional activities carried out in compliance with data protection rules. Thus, without such system configuration, it was not able to ensure what customer data had been processed at every stage, for each of the processing purposes. The DPA ruled that the company was, inter alia, in structural breach of Articles 5(1), 5(2), and 25(1) GDPR. For the DPA, the number of unsolicited calls revealed a serious flaw in the accountability of the controller, as well as in some key elements of the privacy by design criterion (such as security and transparency of processing). The DPA noted that Vodafone's flaws could be easily exploited by unauthorized parties by, for instance, contacting potential customers without complying without prior consent, and decided to impose a fine of 12,251,601 EUR.[171]

3.2. Privacy Preservation in Online Environments and the increasing role of PETs

This section will highlight cases where controllers had to improve privacy preservation in online environments. Some DPAs have started exploring PETs in their guidance to explain to what extent the use of PETs could help controllers comply with the GDPR.[172] However, at the time of writing European DPAs are yet to further develop their common views on PETs in online environments, which should occur in the context of the two upcoming updates of the guidelines on anonymization and on pseudonymization.[173]

In the meantime, some noteworthy enforcement cases regarding the use of specific technologies by controllers and their processors to comply with the GDPR's security requirements reveal that European DPAs focus mainly on technical measures that are explicitly condoned by the GDPR, such as encryption and pseudonymization. In this regard, the Norwegian DPA's recent decision (Case NO3) recommending the use of synthetic data to test information systems under development may mark a turning point in regulators' appetite to take on board synthetic data as a PET.

Case NO3: Synthetic data as a possible avenue to test new systems with personal data[174]

The Norwegian Sports Confederation (NIF) exposed personal data of 3.2 million Norwegians (including minors) online for 87 days due to inadequate security checks during the testing of a new cloud solution for the management of NIF's members. The Norwegian Datatilsynet had no information that unauthorized persons managed to exploit the incident, but nevertheless determined that NIF was lacking robust security measures for testing its systems and had no legal basis for testing a new system with personal data. The DPA observed that processing synthetic data and using fewer categories of personal data could have enabled NIF to test new software solutions for NIF membership administration in a less privacy-intrusive way. This recommendation is also in line with the DPA's guidance for software development with built-in privacy, where testing is an important part.[175] We note, however, that Datatilsynet does not delve into the details of how the controller should carry out the data synthesis process. The DPA decided to impose a NOK 1,250,000 (roughly 109,000 EUR) fine for breaches of Articles 5(1)(a, c, f), 6, and 32 GDPR.

It is disputed in academic circles and amongst data protection regulators whether techniques such as synthetic data enable controllers to achieve irreversible anonymization.[176] Reaching anonymization without significant loss of data utility through the application of technical solutions has been labeled as the "golden Goose of privacy law," because of how challenging of a problem it is.[177]

Indeed, the threshold set up under the GDPR for anonymization of personal data, which differentiates between pseudonymized data, to which the regulation applies (albeit with some flexibility) and anonymized data, which falls outside of the regulation's scope.[178] In assessing whether individuals remain identifiable, Recital 26 GDPR states that the controller should consider "all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person". In this context, the controller is expected to assess objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[179] But

also context matters, since it may reveal new information that could lead to the identification of a natural person.

While there are still no enforcement actions in which DPAs touch on the role PETs can play in pursuing anonymization, other regulators have joined the UK ICO in exploring the topic in various opinion pieces and guidance notes. In its recent DPbD&bD guidance, the Catalan APDCAT seems optimistic that techniques like differential privacy have the potential to anonymize datasets, while expressing reservations about synthetic data's power to achieve such an outcome.[180] On the other hand, the Spanish AEPD has been exploring different PETs in blog posts, providing indications of how the regulator will regard their use in future corrective actions:

- ***Homomorphic encryption*** prevents handing over decryption keys to processors that offer cloud-based services, and as such is a "very interesting privacy by default measure, especially for the processing of special categories of personal data."[181]

- ***Differential privacy*** adds random noise to datasets to enable the extraction of equivalent statistical results, also working as a data protection by design tool.[182]

- ***Secure multiparty computation*** enables the creation of federated data spaces for private-by-design analytics by allowing data to remain in the entities that generate it and undergo processing at source at the request of or in collaboration with third parties.[183]

- ***Zero-knowledge proofs*** (ZKPs) are a set of techniques that allow the implementation of data minimization and access limitations as set out in Article 25 GDPR and can potentially be applied to GDPR-aligned age verification mechanisms. Even if they are considered powerful pseudonymization tools, they may expose individuals to certain risks, such as profiling, exchanges of metadata, and device fingerprinting.[184]

- ***Federated learning*** models for training AI systems, which rely on edge computing to bring the processing to the data instead of the data to the processing, thereby facilitating the implementation of the data minimization principle.[185]

In sum, DPAs are increasingly exploring the potential PETs offer to controllers. In **Case IT2**, the Italian Garante highlighted the importance of keeping data in encrypted form in transit and at rest, as long as the controller relies on state-of-the-art cryptography and applies sound complementary organizational measures, such as keeping decryption keys secure and protected from unauthorized access. We remark that encryption is mentioned in numerous cases we analyzed throughout this report (see **Cases PL4**, **PL6,** and **FI10).** In the context of a French case, the keys used for encrypting the health data were kept out of reach of the online service provider, AWS, to ensure the protection of the data transferred to the latter.[186] Additionally, in a 2021 ruling, the Belgian Administrative Court has determined that using encryption with separate key management can serve as an effective supplementary measure for a Flemish public entity that is utilizing cloud services provided by an affiliate of a US-based company, in addition to the implementation of Standard Contractual Clauses (SCCs) to ensure compliance with the GDPR.[187] On the other hand, the Dutch Data Protection Authority (AP) saw no reason to conduct a further investigation into possible violations of the GDPR by the Medical Research Data Management, a processor acting on behalf of a number of Dutch hospitals, when storing medical data on a cloud platform, being satisfied that the personal data is stored in the Netherlands.[188] Moreover, a decision from the Greek HDPA illustrates how regulators expect controllers to deploy effective anonymization instead of pseudonymization whenever possible to pursue specific processing purposes, such as producing statistics.

Case GR4: Anonymization should be prioritized when processing for statistics[189]

Telecommunications provider Cosmote informed the Greek HDPA that during an audit of its systems, it detected an unauthorized extraction of a file containing personal data of subscribers as a result of a cyber attack. According to the DPA's investigation, Cosmote was storing traffic and location data in its systems for three months in order to detect and correct technical failures and for 12 months for statistical purposes. The file holding data for 12 months was separate to the one being held for three months and was being anonymized. The DPA "enriched" the statistics database with information about customers' subscription plans, age, gender, and average revenue. The HDPA determined that according to the purpose limitation principle under Article 5(1)(b) GDPR, processing for statistical purposes could be considered compatible, provided that appropriate TOMs are implemented in accordance with Article 89(1) GDPR. In the present case, Cosmote pseudonymized data instead of anonymizing it, as it merely sought to minimize the risk of identification and not to eliminate it. For the DPA, and since COSMOTE held the decryption keys, this measure was not sufficient and constituted a violation of Article 25(1) GDPR. This resulted in a fine of 6M EUR, of which 1.3M EUR was due to a breach of Article 25(1) GDPR.

3.3. EdTech: proctoring and virtual learning tools are subject to strict requirements

As we have seen with **Case NO1** concerning the International Baccalaureate in Section 2.2. above, public and private teaching institutions are increasingly relying on new technologies to engage with students for learning and assessment purposes ("EdTech"). This has particularly been the case during the Covid-19 pandemic, as virtual interactions in the school context increased significantly. However, as we will see in this section, institutions have not always embedded DPbD&bD into the systems they developed or deployed, and DPAs in multiple countries used their corrective powers in various scenarios. The vast majority of the cases in this section concern the ways teaching institutions held and monitored distance exams during the Covid-19 pandemic.

Case IT11: Proctoring software collects unnecessary student data[190]

The Italian Garante conducted an investigation into the Luigi Bocconi University's use of a software called "Respondus" — provided by US company Respondus Inc. — to monitor students' remote exams during the Covid-19 crisis. The software captured video images in order to detect unusual and suspicious behaviors, used profiling to produce and send warning signals, and flagged the incidents to the supervisor, who later assessed the case to decide whether the student's exam should be invalidated or not. The Garante found that the software was capturing unnecessary information about the students, including data that could reveal aspects about students' private life (e.g., applications in use on the student's terminal). Furthermore, the data storage period of five years plus twelve months after the termination of an eventual legal dispute was considered to be too long, as it was not proportionate to the purpose of ensuring the regularity of exams. For the DPA, these amounted to breaches of Articles 5(1)(c), 5(1)(e), and 25 of the GDPR. It is also worth noting that the Garante explicitly mentioned the EDPB guidelines on DPbD&bD to state that the controller's obligations also apply when the latter uses third-party products or services, as was the case of the Respondus proctoring software. The DPA imposed a number of corrective measures and a fine of 200,000 EUR.[191]

On the other hand, **Case DK2** offers an example of a compliant use of proctoring software by a University. The Danish Datatilsynet investigated the use of the "ProctorExam" solution by the IT University of Copenhagen's (ITU) to monitor virtually-held exams during the Covid-19 pandemic and detect potentially fraudulent acts by students during the examination process. For the DPA, the program was in line with the GDPR, in particular with the DPbD&bD rules set out in Article 25 GDPR. This compliance was achieved because:

- ITU had searched the market and chose the least intrusive solution (ProctorExam) which made video, audio, and screen recordings (including of students' browsing behavior) only during the time the exam was in progress;
- The software was easy to install and uninstall, and did not require more data access permissions for the examinees' computers than relevant and necessary;
- The recordings were continuously transmitted from the examinees' computers in an encrypted fashion, using secure protocols, which also applied when the recordings were subsequently accessed by the relevant staff;
- The recordings were stored within the EU on servers in Frankfurt, only for 21 days and encrypted with Amazon S3 server-side encryption, AES-256; and
- Access to the recordings was limited to what was necessary, and access by and transmission between authorized employees took place on the employees' local work computers via a secure web interface with appropriate encryption.

While the DPA still recommended ITU to implement two-factor authentication for access control, it overall applauded the choices made by ITU to configure the browser extension in question in such a way that information about the examinees that is not relevant in relation to monitoring the exam, including search history, is not collected.[192]

Another cluster of cases concentrate on virtual learning methods, where, again, DPAs expect controllers to deploy both robust TOMs to protect students' and professors' data protection rights. This requires, first and foremost, that controllers properly assess the risks that cloud-based tools for learning purposes present to such rights and freedoms, in line with DPbD&bD.

Case GR5: Use of virtual learning platform has significant risks for users relying on personal devices, which should be explained and addressed[193]

The Hellenic Ministry of Education and Religious Affairs implemented virtual learning using the platform Webex for primary and secondary school students during the Covid-19 pandemic. The platform collected data about users and their activity on the device for statistical analysis. The Greek HDPA issued two opinions in which it found that the ministry had put forward specific TOMs to ensure that the data subjects' rights were being safeguarded, but not optimally. For the DPA, the controller failed to consider and systematically address the risks arising from the use of personal devices by students and teachers to access the platform. Moreover, user identity checks were considered insufficient as a security measure due to lack of training of those using it and it should have been complemented by providing teachers and pupils with more robust information and codes of conduct. The DPA recommended that the ministry organize awareness-raising activities that focus on explaining risks associated with new tools and respecting the personal data of students and third parties. The DPA determined that the ministry breached Article 25(1) GDPR and gave it two months to remedy the violation.

Case FI4: Free cloud-based learning tools should be subject to strict risk assessments[194]

A complainant brought to the attention of the Finnish Data Protection Ombudsman the use of Google's G Suite (now Workspace) program as the primary electronic learning environment in Finnish schools during the exceptional circumstances caused by Covid-19. Besides not considering the processing as justified under the fulfillment of public tasks lawful ground, as mentioned in Section 2.2.a.i., the DPA pointed out that the encryption method used (MD5) was outdated since there were easily-available softwares that could crack the encryption algorithm. The DPA also noted that when a school uses free programs in education, it should first properly and wholly assess their risks for data subjects' rights, which the controller did not do. Thus, having detected a breach of Article 25 GDPR, the DPA ordered the controller to bring its processing into compliance with the GDPR, notably after assessing whether additional safeguards should be introduced for data transfers related to the use of the program.

4. CONCLUSION

Our analysis shows that some DPAs focus more on specific elements of Article 25 GDPR than others when enforcing the law. This is not surprising, considering the contextual nature of the DPbD&bD obligations and how generous is the wording of the provision with all the elements that should be embedded in the design of processing activities. For instance, in Finland the focus has been on privacy by default under Article 25(2) GDPR and data minimization, whereas in Poland the DPA has focused more on the responsibility of the controller concerning the monitoring of its processors and security measures.

Our analysis also highlights how DPAs have divergent interpretations on the arguably preventive nature of Article 25 GDPR. In a few cases, DPAs were reluctant to find a violation of the article if an incident constituted an isolated case or when no principle of Article 5 GDPR had been violated. However, they did not hesitate to sanction controllers where isolated incidents revealed structural compliance shortcomings with DPbD&bD, as **Cases IS3**, **RO4,**[195] and **BG-CR-1** illustrate.

DPAs also hesitate in many instances to enforce Article 25 where processing of personal data, a data breach, or a violation of data subjects' rights is yet to occur. This happened in **Case AT2**, where the Austrian DPA refused to act on a complaint from a citizen who claimed that the lack of appropriate TOMs in a public repository exposed his personal data to third-parties, but failed to demonstrate that undue access had occurred. The Finnish DPA in **Case FI5** also ruled that a company that was asking for health data of its clients would be processing sensitive personal data without having a legal basis and would be in breach of Articles 5(1)(c) and 25 of the GDPR, but since no personal data had actually been collected, it issued just a warning. Finally, Austria's Supreme Court determined that since the rules provided in Article 25(2) GDPR only oblige the controller to take certain measures, a contractual clause that provides for unlawful processing of personal data cannot in and of itself contradict this provision.

Case AT-CR-1: Contractual clauses do not breach DPbD&bD[196]

This case brought to the Austrian Supreme Court concerns a complaint made by an Austrian consumer rights organization (VKI) against two car rental companies that allegedly used unlawful general terms and conditions and thus violated Article 25(2) GDPR. This case is particularly relevant given that the court determined — overruling the lower court's decision — that the judicial action constituted "a [merely] theoretical complaint against the data processing by the defendant." The court took the view that "since the rules provided for in Article 25(2) GDPR only obligate the controller to take certain measures, a contractual clause [in and of itself] cannot contradict this provision. The action could therefore only be interpreted as a complaint against the data processing described in the clauses."[197] The Austrian Supreme Court also referred a question to the CJEU requesting a preliminary ruling on whether organizations entitled to file class actions under national consumer protection law can also file such actions concerning data protection cases. The question seems to have been answered in another CJEU ruling in the meantime, so it is likely that the Austrian Supreme Court will decide on the merits of the case soon.[198]

At the other extreme, we observe that certain DPAs ruled in favor of applying Article 25 GDPR preventively, before further or more serious GDPR breaches occurred, or even before planned data processing took place. As we saw in **Cases BE1** and **IT4**, the Belgian and Italian DPAs ruled that even if no processing has occurred and no data protection principle has been violated, Article 25 can still be applied. For the Irish DPA in **Case IE1**, Article 25 calls on controllers to address "potential risks," "possible harm," and "exposure to danger," and thus, empowers DPAs to initiate corrective actions in case of failures in that regard.

The Irish DPC is not alone in outlining the requirements under Article 25 GDPR that mandate controllers to act proactively in detecting and tackling potential breaches of the GDPR that arise from planned processing. Such type of assessment is not only required in situations where a DPIA is mandatory, but also the criteria laid out under EDPB guidelines on DPIAs may prove useful for controllers when carrying out risk assessments under Articles 24 and 25 GDPR. In **Case IT7,** the Italian Garante noted that the controller should verify compliance with the GDPR before and throughout the processing by applying an appreciable and proactive approach rather than a reactive one. In line with this spectrum of cases, an advisory opinion from the German State of Hamburg's DPA explores the extent to which Article 25 GDPR is obligatory for the controller, even if individuals may waive the implementation of certain TOMs via informed consent.[199]

We have also identified that even the same DPA may not apply Article 25 GDPR consistently. More specifically, the Belgian DPA had the opportunity to rule on cases of unlawful processing of personal data for electoral purposes several times. However, only in **Case BE3** did the Belgian DPA's Litigation Chamber find a violation of Article 25 GDPR, whereas in four other cases it imposed administrative fines for non-compliance with other provisions only, such as the purpose limitation principle under Article 5(1)(b) GDPR.

From our case-law sweep and analysis, enforcement cases across Europe (such as **Case PL3**) show that DPAs expect controllers to ensure compliance with Article 25 GDPR through a combination of TOMs, without establishing predominance of one type of measureover others. Despite the fact that both Articles 25 and 32 refer to the cost of implementation of specific TOMs as one of the factors that controllers should consider when selecting and implementing measures, DPAs do not seem sympathetic to cost-based justification for not deploying effective TOMs, as **Case IT2** illustrates. Robust and secure information systems for processing personal data may still be vulnerable to attacks and data leakage if the appropriate business and human processes and training are not in place, as **Case HU1** on the use of an employee account by another employee during the former's sick leave demonstrates.

Another important finding of our research is that *DPAs require the TOMs chosen by controllers to be appropriate to the identified risks, but also to effectively prevent the occurrence of GDPR violations*, such as data breaches. This is made clear in **Cases IE2** and **PL7**. Nonetheless, we also encountered reluctance from DPAs in a few cases about stating what would be an appropriate TOM or what exactly was not in conformity with Article 25 GDPR. For instance, in a decision concerning social media platform TikTok, the Italian DPA shies away from providing specific guidance on GDPR-compliant age verification mechanisms, while declaring that the platform's practices were not good enough.

Case IT12: Self-declaration and user behavior monitoring are not appropriate age verification mechanisms[200]

The Italian Garante imposed restrictions on TikTok's processing of personal data related to users under 13 in January and February 2021 due to the lack of suitable age verification systems. The Garante found that self-declaration of age and user behavior verification were not sufficient measures to exclude children from using the platform and did not respect the accountability principle and Article 25 GDPR. As a result, the Garante ordered TikTok to implement suitable barrier measures and temporarily limit processing of personal data of users whose age it could not verify. The measures should prevent minors aged 13 or under that lack legal guardian consent from accessing the platform and include a clear notice highlighting that the app is for users over 13. Nonetheless, the Garante did not provide specific guidance for valid age verification mechanisms.[201]

Our research shows that European DPAs are generally not ready to apply data protection requirements to PETs in enforcement cases, with one decision from the Norwegian DPA constituting the exception. At this stage, regulators are more prone to advance their positions in multiple guidelines and opinion pieces, setting some expectations for controllers that develop and purchase these new technologies for GDPR compliance purposes. Overall, until there is more alignment in European DPAs' views about the potential benefits and shortcomings of different PETs, authorities who exercise corrective powers more often evaluate and suggest the implementation of technical measures that are explicitly mentioned in the GDPR — such as encryption and pseudonymization — and that have been the subject of debate over many years under the auspices of the old Data Protection Directive.

After having analyzed over 130 cases and several relevant guidelines and academic papers, it is clear that DPAs are willing to enforce Article 25 GDPR and the provision is thus "capable of real bite."[202] This finding contradicts the belief that the nature and text of Article 25 is too vague to be applied in individual cases, non-implementable, and non-enforceable in practice. DPAs often detect shortcomings of controllers' TOMs and do not shy away from outlining some appropriate and state-of-the-art measures that they should have implemented to become or remain GDPR compliant.[203] We also note that some of the highest fines imposed by DPAs to date have elements of non-compliance with Article 25 GDPR, such as in the cases of the Irish DPC's decisions concerning public-by-default settings and user search tools in two social media platforms, which opened the door to data scraping and exposed minors to significant risks (**Cases IE1** and **IE2**).

Regardless of the high expectations that regulators have with regards to the due diligence controllers ought to conduct when applying Article 25 in their daily operations, there is anecdotal evidence beyond the enforcement actions analyzed for this report that controllers are lagging behind. Consensual audits from the UK ICO on 11 Multi Academy Trusts (MATs) showed that 72% of them had not documented or explained their data minimization and pseudonymization measures, as required by Article 25 of the GDPR, and 54% of them had not integrated core privacy considerations into their project management and risk management methodologies and policies.[204]

That said, some aspects of practical compliance with Article 25 GDPR would benefit from further clarifications from the EDPB, for instance in its upcoming guidance on anonymization and

pseudonymization. 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. Future EDPB binding decisions or CJEU rulings in response to preliminary questions received from national courts could settle divergences that have emerged from courts' and DPAs' enforcement records, such as whether Article 25 applies regardless of the existence of processing and whether a breach of the provision entitles individuals to compensation under Article 82 GDPR.

ANNEX I — LIST OF CASES

Court Rulings

Court of Justice of the EU (CJEU)

Case CJEU1: Joined Cases WM (C-37/20), Sovim SA (C-601/20), Grand Chamber, November 22, 2022, ECLI:EU:C:2022:912.

Austria (AT)

Case AT-CR-1: Austrian Supreme Court, Case: 6Ob77/20x of November 25, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20201125_OGH0002_0060OB00077_20X0000_000.

Belgium (BE)

Case BE-CR-1: Cour d' appel Bruxelles, Case: 2020/AR/1333 of January 27, 2021, available at https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-27-januari-2021-van-het-marktenhof-ar-1333-beschibaar-in-het-frans.pdf.

Bulgaria (BG)

Case BG-CR-1: Supreme Administrative Court of the Republic of Bulgaria — Fifth Division, case No. 6307/27.06.2022 of June 27, 2022, available at https://info-adc.justice.bg/courts/portal/edis.nsf/e_act.xsp?id=1941175&code=vas.

France (FR)

Case FR-CR-1: Conseil d'État — 1ère — 4ème chambres réunies, no 428451 of November 25 2020, available at https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042570046?tab_selection=cetat&searchField=ALL&query=428451&searchType=ALL&juridiction=TRIBUNAL_CONFLIT&juridiction=CONSEIL_ETAT&juridiction=COURS_APPEL&juridiction=TRIBUNAL_ADMINISTATIF&sortValue=DATE_DESC&pageSize=10&page=1&tab_selection=cetat#cetat.

Germany (DE)

Case DE-CR-1: LG Heilbronn, Bu 8 O 131/22, January 13, 2023, available at https://beck-online.beck.de/Dokument?vpath=bibdata%2Fents%2Fbeckrs%2F2023%2Fcont%2Fbeckrs.2023.330.htm&anchor=Y-300-Z-BECKRS-B-2023-N-330.

Case DE-CR-2: LG Stuttgart, Case No 53 O 95/22 of January 26, 2023, available at https://lnkd.in/euqZrMTS.

Case DE-CR-3 Munich Higher Regional Court, final judgment of December 8, 2020 – 18 U 2822/19, available at https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2020-N-34203.

Case DE-CR-4: Bundesgerichtshof, Judgement of January 27, 2022 — III ZR 3/21.

Poland (PL)

Case PL-CR-1: Judgment of the Provincial Administrative Court in Warsaw, II SA/Wa 2559/19 of September 3, 2020, available at https://orzeczenia.nsa.gov.pl/doc/2F881CED73.

DPA Decisions

Austria (AT)

Case AT1: Datenschutzbehörde, Case DSB-D123.822/0005-DSB/2019 of July 23, 2019, available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20190723_DSB_D123_822_0005_DSB_2019_00/DSBT_20190723_DSB_D123_822_0005_DSB_2019_00.html.

Case AT2: Datenschutzbehörde, Case GZ: DSB-D123.070/0005-DSB/2018 of September 13, 2018, available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180913_DSB_D123_070_0005_DSB_2018_00/DSBT_20180913_DSB_D123_070_0005_DSB_2018_00.pdf.

Belgium (BE)

Case BE1: APD/GBA, Numéro de dossier: DOS-2019-0549, Case: 82/2020, December 23, 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-82-2020.pdf.

Case BE2: APD/GBA Numéro de dossier: DOS-2020-03432, Case: 85/2022 of May 25, 2022, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-85-2022.pdf.

Case BE3: APD/GBA, N° de dossier : DOS-2019-02974, Case: 53/2020 of September 1, 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-53-2020.pdf.

Case BE4: APD/GBA, Numéro de dossier : DOS-2019-04412, Case: 74/2020 of November 24, 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-74-2020.pdf.

Case BE5: APD/GBA, Dossiernummer: DOS-2019-05244, Case: 127/2022 of August 19, 2022, available at https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-127-2022.pdf.

Case BE6: APD/GBA, Numéro de dossier : DOS-2020-04002, Case: 21/2022 of February 2, 2022, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf See also the press release, available at https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr.

Case BE7: APD/GBA, Numéro de dossier : DOS-2019-04798, Case: 047/2021 of January 20, 2021 available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-04-2021.pdf.

Denmark (DK)

Case DK1: Datatilsynet, Journal number: 2019-442-4365 of April 22, 2020, available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/apr/kolding-kommune-havde-ikke-truffet-passende-tekniske-og-organisatoriske-foranstaltninger.

Case DK2: Datatilsynet, Journal number: 2020-432-0034 of January 26, 2021, available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen.

Finland (FI)

Case FI1: Tietosuojavaltuutetun toimisto, Case 531/161/20 1 (16), available at https://tietosuoja.fi/documents/6927448/22406974/Ty%C3%B6ntekij%C3%B6iden+sijaintitietojen+k%C3%A4sittely+ja+vaikutustenarviointi.pdf/2d04e545-d427-8a0d-3f4d-967de7b428ac/Ty%C3%B6ntekij%C3%B6iden+sijaintitietojen+k%C3%A4sittely+ja+vaikutustenarviointi.pdf.

Case FI2: Tietosuojavaltuutetun toimisto, Diary number: 1150/161/2021 of December 7, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211183.

Case FI3: Tietosuojavaltuutetun toimisto, Diary number 6097/161/21 of May 9, 2022, available at https://finlex.fi/fi/viranomaiset/tsv/2022/20221483. See also the press release, available at https://tietosuoja.fi/-/otavamedialle-seuraamusmaksu-puutteista-tietosuojaoikeuksien-toteutuksessa.

Case FI4: Tietosuojavaltuutetun toimisto, Diary number 1509/452/18 of December 30, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211503.

Case FI5: Tietosuojavaltuutetun toimisto, Diary number: 2368/182/20 of August 6, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211004.

Case FI6: Tietosuojavaltuutetun toimisto, Diary number 8493/161/21 of December 16, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211303.

Case FI7: Tietosuojavaltuutetun toimisto, Diary number: 137/161/2020 of May 18, 2020, available at https://finlex.fi/fi/viranomaiset/tsv/2020/20200583.

Case FI8: Tietosuojavaltuutetun toimisto, Diary number: 834/532/18 of November 9, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211225#OT2.

Case FI9: Tietosuojavaltuutetun toimisto, Diary number: 8211/161/19 of November 9, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211223.

Case FI10: Tietosuojavaltuutetun toimisto, Diary number: 4282/161/21 of December 16, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211244.

Case FI11: Tietosuojavaltuutetun toimisto, Diary number: 6813/171/21 of May 31, 2022, available at https://finlex.fi/fi/viranomaiset/tsv/2022/20221463.

Case FI12: Tietosuojavaltuutetun toimisto, Diary number:2984/182/2019 of June 26, 2020, available at https://finlex.fi/fi/viranomaiset/tsv/2020/20200601.

France (FR)

Case FR1: CNIL, Délibération SAN-2022-020 of November 17, 2022, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046562676.

Germany (DE)

Case DE1: BinBDI, case 711.412.1 of November 5, 2019, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.

Greece (GR)

Case GR1: HDPA, case 31/2019 of October 7, 2019, available at https://www.dpa.gr/sites/default/files/2019-12/31_2019anonym%20%281%29.pdf.

Case GR2: HDPA, Case 13/2021 of April 17, 2021, available at https://www.dpa.gr/sites/default/files/2021-04/13_2021anonym.pdf.

Case GR3 HDPA, Case 20/2021 of May 12, 2021, available at https://www.dpa.gr/sites/default/files/2021-05/20_2021anonym.pdf.

Case GR4: HDPA, Case 04/2022 of January 27, 2022, available at https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf.

Case GR5: HDPA 50/2021 of November 16, 2021, available at https://www.dpa.gr/sites/default/files/2021-11/50_2021anonym.pdf.

Hungary (HU)

Case HU1: Hungarian National Authority for Data Protection and Freedom of Information, Case NAIH/2019/769/ (NAIH/2018/5997/H.) of October 15, 2019, available at https://www.naih.hu/files/NAIH-2019-769-hatarozat.pdf.

Case HU2: Hungarian National Authority for Data Protection and Freedom of Information, Case No. NAIH/2020/2204/8 Cipőkereskedelmi Korlátolt Felelősségű Társaságnak Deichmann, issued September 3, 2020, available at https://www.naih.hu/files/NAIH-2020-2204-8-hatarozat.pdf.

Case HU3: Hungarian National Authority for Data Protection and Freedom of Information, Case No. NAIH-85- 3/2022 Budapest Bank, issued February 8, 2022, available at https://naih.hu//hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei.

Case HU4: Hungarian National Authority for Data Protection and Freedom of Information, case NAIH-924-10/2021 of June 18, 2021, available at https://www.naih.hu/hatarozatok-vegzesek?download=405:erintetti-jogok-biztositasanak-kotelezettsege-nem-ugyfel-erintettek-reszere.

Iceland (IS)

Case IS1: PersónuVernd, Case no. 2020092451 of January 12, 2022, available at https://www.personuvernd.is/urlausnir/vinnsla-landsbankans-a-personuupplysingum-ekki-i-samraemi-vid-log.

Case IS2: PersónuVernd, Case no. 2020010428 of March 10, 2020, available at https://www.personuvernd.is/urlausnir/oryggisbrestur-hja-saa-sektarakvordun.

Case IS3 PersónuVernd, Case of March 10, 2020 available at https://www.personuvernd.is/urlausnir/nr/2885%20.

Case IS4: PersónuVernd, Case no. 2020010656 of May 3, 2022 available at https://www.personuvernd.is/urlausnir/vinnsla-barnaverndarnefndar-hafnarfjardar-a-personuupplysingum-ekki-i-samraemi-vid-log.

Case IS5: PersónuVernd, Case no. 2021040879 of December 20, 2021, available at https://www.personuvernd.is/urlausnir/akvordun-um-notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur.

Ireland (IE)

Case IE1: Irish DPC, DPC Inquiry Reference: IN-20-7-4 of September 2, 2022, available at https://edpb.europa.eu/system/files/2022-09/in-20-7-4_final_decision_-_redacted.pdf.

Case IE2: Irish DPC, Reference: IN-21-4-2 in the matter of Meta Platforms Ireland Ltd. (Formerly Facebook Ireland Ltd.) of November 25, 2022, available at https://www.dataprotection.ie/sites/default/files/uploads/2022-12/Final%20Decision_IN-21-4-2_Redacted.pdf See also the press release, available at https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

Case IE3: Irish DPC, decision of September 14, 2022, available at https://www.dataprotection.ie/sites/default/files/uploads/2023-01/Airbnb%20Ireland%20UC%20IN-21-3-1%20Redacted%20Decision%20EN.pdf.

Case IE4: Irish DPC, DPC Case Reference: IN-19-7-2 of March 23, 2021, available at https://www.dataprotection.ie/sites/default/files/uploads/2021-05/Redacted_23.03.2021_Decision_IN-19-7-2.pdf.

Italy (IT)

Case IT1: Garante, Ordinanza ingiunzione nei confronti di Roma Capitale — 22 luglio 2021 [9698724], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9698724.

Case IT2: Garante, Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. — 10 giugno 2021 [9685922], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685922.

Case IT3: Garante, Provvedimento del 25 febbraio 2021 [9556958], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958.

Case IT4: Garante, Ordinanza ingiunzione nei confronti di Iliad Italia S.p.A. — 9 luglio 2020 [9435807], available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435807.

Case IT5: Garante, Ordinanza ingiunzione nei confronti di Azienda sanitaria universitaria Friuli Centrale — 26 maggio 2022 [9790365], availabe at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9790365.

Case IT6: Garante, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. — 22 luglio 2021 [9685994] available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

Case IT7: Garante, Ordinanza ingiunzione nei confronti di Enel Energia S.p.a. — 16 dicembre 2021 [9735672], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9735672.

Case IT8: Garante, Ordinanza ingiunzione nei confronti di La Prima S.r.l. — 16 settembre 2021 [9705632], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9705632.

Case IT9: Garante, Ordinanza ingiunzione nei confronti di Wind Tre S.p.A. — 9 luglio 2020 [9435753], available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435753.

Case IT10: Garante, Ordinanza ingiunzione nei confronti di Vodafone — 12 novembre 2020 [9485681], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681.

Case IT11: Garante, Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano — 16 settembre 2021 [9703988], availabe at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988.

Case IT12: Garante, Provvedimento del 25 marzo 2021 [9574709], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9574709.

Case IT13: Garante, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. — 10 giugno 2021 [9675440], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.

Case IT14: Garante, Ordinanza di ingiunzione nei confronti di Fondazione Policlinico Tor Vergata di Roma — 21 aprile 2021 [9591223], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9591223.

Case IT15: Garante, Ordinanza ingiunzione nei confronti di Centro di Medicina preventiva s.r.l. — 16 dicembre 2021 [9739609], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9739609.

Case IT16: Garante, Ordinanza ingiunzione nei confronti di Fastweb S.p.A. — 25 marzo 2021 [9570997], available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9570997.

Case IT17: Garante, Prescriptive and sanctioning measure against Ediscom SpA — 23 February 2023 [9870014], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014.

Norway (NO)

Case NO1: Datatilsynet, Ref No 20/03087-14 of August 7, 2020, available at https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf.

Case NO2: Datatilsynet, Ref No 18/04147-23/KBK of February 25, 2020, available at https://www.datatilsynet.no/contentassets/0c61777547e74a6e90ad4555a1728869/varsel-om-vedtak-om-palegg-og-overtredelsesgebyr_statens-vegvesen.pdf.

Case NO3: Datatilsynet, May 5, 2021, available at https://www.datatilsynet.no/contentassets/27d554561ceb4e77ad22b54fad5bfe0e/vedtak-om-overtredelsesgebyr-til-norges-idrettsforbund.pdf.

Poland (PL)

Case PL1: UODO, DKN.5130.2215.2020 of January 19, 2022, available at https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020.

Case PL2: UODO, DKN.5130.1354.2020, December 17, 2020, available at https://uodo.gov.pl/decyzje/DKN.5130.1354.2020.

Case PL3: UODO, DKN.5101.25.2020 of November 12, 2020, available at https://uodo.gov.pl/decyzje/DKN.5101.25.2020.

Case PL4: UODO, DKN.5130.2559.2020 of December 9, 2021, available at https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020%20.

Case PL5: Judgment of the Provincial Administrative Court in Warsaw, II SA/Wa 2559/19 of September 3, 2020 available at https://orzeczenia.nsa.gov.pl/doc/2F881CED73.

Case PL6: UODO, DKN.5131.22.2021 of July 13 2021, available at https://www.uodo.gov.pl/decyzje/DKN.5131.22.2021.

Case PL7: UODO, DKN.5130.2815.2020 of January 11, 20210, available at https://www.uodo.gov.pl/decyzje/DKN.5130.2815.2020. With a similar subject-matter, rationale, and corrective actions.

Case PL8: UODO, DKN.5112.1.2020 of December 3, 2020, available at https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020.

Case PL9: UODO, DKN.5131.56.2021 of June 14, 2022, available at https://www.uodo.gov.pl/decyzje/DKN.5131.56.2021.

Case PL10: UODO, DKN.5131.11.2022 of June 23, 2022, available at https://www.uodo.gov.pl/decyzje/DKN.5131.11.2022.

Case PL11: UODO, DKN.5131.2.2022 of June 1, 2022, available at https://www.uodo.gov.pl/decyzje/DKN.5131.2.2022.

Romania (RO)

Case RO1: ANSPDCP, case of August 4, 2020, the press release is available at https://www.dataprotection.ro/?page=Comunicat_Presa_01_09_2020&lang=ro.

Case RO2: ANSPDCP, Case of November 16, 2022, the press release is available here https://www.dataprotection.ro/?page=Comunicat_Presa_16_11_2022&lang=ro.

Case RO3: ANSPDCP, case of June 27, 2019, available at https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro.

Case RO4: ANSPDCP, case of December 10, 2019, available here, https://www.dataprotection.ro/?page=Alta_amenda_pentru_incalcarea_RGPD_2020_1&lang=ro.

Spain (ES)

Case ES1: AEPD Procedimiento Nº: PS/00003/2021 of February 25, 2022, available at https://www.aepd.es/es/documento/ps-00003-2021.pdf.

Case ES2: AEPD, Procedimiento Nº: PS/00120/2021 of July 26, 2021 available at https://www.aepd.es/es/documento/ps-00120-2021.pdf.

Case ES3: AEPD Procedimiento Nº: PS/00236/2020 — May 4, 2021, available at https://www.aepd.es/es/documento/ps-00236-2020.pdf See also the EDPB press release, available at https://edpb.europa.eu/news/national-news/2021/spanish-dpa-imposes-fine-1500000-euros-epd-energia-sau-two-infractions-gdpr_en.

United Kingdom (UK)

Case UK1: Information Commissioner's Office, INV/0561/2021 of June 7, 2022, available at https://ico.org.uk/media/action-weve-taken/reprimands/4023124/bolton-at-home-reprimand.pdf.

ANNEX II — COMPARATIVE OVERVIEW OF DPA ENFORCEMENT ACTIONS ACROSS THE EEA

Country	Number of DPA decisions where Article 25 GDPR was mentioned	Total amount of fines
Austria	2	0 EUR
Belgium	6	326,500 EUR
Denmark	2	0 EUR
Finland	12	733,000 EUR
France	1	800,000 EUR
Germany	1	14,500,000 EUR
Greece	5	9,675,000 EUR
Hungary	4	782,721 EUR
Iceland	5	28,646 EUR
Ireland	4	670,000,000 EUR
Italy	17	67,631,046 EUR
Norway	2	352,327 EUR
Poland	12	2,459,841 EUR
Romania	4	158,500 EUR
Spain	3	4,320,000 EUR
United Kingdom	1	0 EUR

REFERENCES

1 Regulation (EU) 2016/679 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) [2016] OJ L 119/1

2 L JASMONTAITE, I KAMARA, G. Z. FORTUNA, S LEUCCI, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' [2018] 4(2) European Data Protection Law Review 168 — 189, <https://doi.org/10.21552/edpl/2018/2/7>

3 L BYGRAVE, *The EU General Data Protection Regulation (GDPR) – A Commentary/Update of Selected Articles*, Oxford University Press, 2021, p. 118-122, available at <https://ssrn.com/abstract=3839645>.

4 L BYGRAVE, 'Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements' [2017] 4 (2) Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo 106 <DOI:10.18261/issn.2387-3299-2017-02-03 >

5 The Italian DPA issued an order against OpenAI, blocking ChatGPT in Italy. The Garante found a violation of Articles 13, 6, 5.1.d and 8 of the GDPR. Article 25 GDPR was referred when the Garante quoted all the GDPR articles that were breached without, however, further explanation: the order of March 31,2023 is available here https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847

6 APDCAT, Privacy by design and privacy by default, A guide for developers, Guides collection. No. 7, February 2023, available at https://apdcat.gencat.cat/en/documentacio/guies_basiques/Guies-apdcat/la-privacitat-des-del-disseny-i-la-privacitat-per-defecte.-guia-per-a-desenvolupadors/; AEPD, *Guía de Privacidad desde el Diseño*, October 2019, available at https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf. AEPD, *Guía de Privacidad desde el Diseño*, October 2020, available at https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf, The CNIL (French DPA) published in 2020 a GDPR guide for developers providing guidance on how to implement the requirements of the GDPR in software development projects and emphasizing the importance of DPbyD&D, available at https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers , 2019; Data protection by design and default ICO (UK DPA) website post, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/; Privacy in the product design lifecycle ICO (UK DPA) website post, available at https://ico.org.uk/for-organisations/privacy-in-the-product-design-lifecycle/; Guidelines 4/2019 on Article 25 Data Protection by Design and by Design, EDPB, Oct. 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. The Norwegian data protection authority (Datatilsynet) has produced guidance on how software developers can implement data protection by design and by default, available at https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/.

7 A CAVOUKIAN, *Privacy by Design The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2011, <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf >

8 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel, *Resolution on Privacy by Design* October, 2010 <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf >

9 FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers,* 2012, pp. 22-34 <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf >

10 According to BYGRAVE, note 4, since Article 25 is not completely aligned to the norm of "privacy by design", as it is more wide-ranging than typical "fair information practices" prescribed in US laws, it is advisable to not use 'DPbD&bD' and 'privacy by design' interchangeably. See also L JASMONTAITE et al, note 2, emphasizing that DPbD&bD is a legal obligation, the noncompliance with which is sanctioned with fines.

11 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

12 Modernized Convention for the protection of individuals with regard to the processing of personal data [Convention 108+],Council of Europe, June 2018, article 10(2), available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

13 Ibid article 10(2).

14 Article 20 and Recital 53 of Directive (EU) 2016/680 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 offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

15 *I v Finland*. Appl. No. 20511/03, Judgment of 17 July 2008, para 36

16 The term is used by Advocate-General Kokott in Case C-110/10 P, *Solvay*, Opinion of 14 April 2011, ECLI:EU:C:2011:257, para. 95. The homogeneity clause can be found in EUCFR Article 52(3).

17 Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of 13 May 2014, ECLI:EU:C:2014:317 and joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, Judgment of 8 April 2014, ECLI:EU:C:2014:238.

18 L BYGRAVE, '*Data Protection by Design and by Default'* [January 2023], The Oxford Encyclopedia of EU Law [OEEUL], January 2023, available at <https://opil.ouplaw.com/display/10.1093/law-oeeul/law-oeeul-e138 >.

19 ISO 31700-1:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*, available at https://www.iso.org/standard/84977.html.

20 D DE CICCO, L VRANESEVIC, C HELLEPUTTE, 'ISO 31700: The Latest Tool to Operationalize (GDPR) Privacy by Design Compliance?', Privacy World 2 February, 2023, available at <https://www.privacyworld.blog/2023/02/iso-31700-the-latest-tool-to-operationalize-gdpr-privacy-by-design-compliance/>.

21 L BYGRAVE, note 4, pp. 117-119.

22 I RUBINSTEIN and N GOOD, 'The trouble with Article 25 (and how to fix it): the future of data protection by design and default' [2020] 10(1) International Data Privacy Law, p. 37-56.

23 L JASMONTAITE et al, note 2.

24 EDPB, note 6, p. 30.

25 M VEALE, R BINNS, J AUSLOOS, 'When data protection by design and data subject rights clash' [2018] 8(2) International Data Privacy Law 105-123 <https://doi.org/10.1093/idpl/ipy002 >.

26 M VEALE et al, note 37.

27 ENISA, *Engineering Personal Data Sharing,* January 27, 2023, available at https://www.enisa.europa.eu/publications/engineering-personal-data-sharing.

28 J H HOEPMAN, *Privacy Design Strategies (The Little Blue Book)*, April 2022, <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>. In his book, Hoepman also cites The Privacy design patterns database, which may be consulted at <https://privacypatterns.org>.

29 EDPB, Work Programme 2023/2024, February 22, 2023, available at https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-2023-2024_en.

30 ARTICLE 29 DATA PROTECTION WORKING PARTY, 0829/14/EN WP216, Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf .

31 ICO, Chapter 5: Privacy-enhancing technologies (PETs), September 2022, available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/.

32 Proposal for a Regulation on European statistics on population and housing, COM(2023) 31 final, amending Regulation (EC) No 862/2007 and repealing Regulations (EC) No 763/2008 and (EU) No 1260/2013, January 2023, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2023:31:FIN. Article 13 of the Proposal favors the sharing of statistical data based on PETs that are specifically designed to implement the principles of the GDPR, whereas Article 14 tasks the Commission and EU Member-States to test and assess the fitness of relevant PETs for secure data sharing. In its recent Opinion on the Proposal, the EDPS notes the role of PETs "as enablers of data sharing which is both privacy friendly and socially beneficial", as well as their link to the principles of DPbD&bD. See EDPS, Opinion 8/2023 on the Proposal for a Regulation on European statistics on population and housing, March 16, 2023, available at https://edps.europa.eu/system/files/2023-03/23-03-16_opinion_european_statistics_and_housing_en.pdf

33 Irish DPC, DPC Inquiry Reference: IN-20-7-4 of September 2, 2022, available at https://edpb.europa.eu/system/files/2022-09/in-20-7-4_final_decision_-_redacted.pdf.

34 Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, adopted on 28 July 2022, available at https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf.

35 During the discussions about DPbD&bD, both the Commission's initial GDPR Proposal and the Council's General Approach imposed duties solely on controllers, whereas the Parliament wished to extend obligations to processors as well. After the negotiations between the EU's co-legislators, the more limited scope prevailed. See L BYGRAVE, note 4.

36 See subsection 1.2 above on the limitations of Article 25 GDPR. However, the EU legislator intends to address this gap through initiatives such as the Cyber Resilience Act. Moreover, we note that developers and producers of information systems (such as AI systems) may assume the role of controllers or processors under the GDPR if they process personal data in the context of the developments, improvement, and support of AI systems. See S BARROS VALE, *GDPR and the AI Act Interplay: Lessons from FPF's ADM Case Law Report*, FPF, November 3, 2022, available at https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/.

37 APD/GBA, Numéro de dossier: DOS-2019-0549, Case: 82/2020, December 23, 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-82-2020.pdf.

38 Garante, Ordinanza ingiunzione nei confronti di Roma Capitale — 22 luglio 2021 [9698724], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9698724.

39 EDPB, note 6, p. 10.

40 UODO, DKN.5130.2215.2020 of January 19, 2022, available at https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020.

41 UODO, DKN.5130.1354.2020, December 17, 2020, available at https://uodo.gov.pl/decyzje/DKN.5130.1354.2020.

42 L JASMONTAITE et al, note 2.

43 Data controllers are required to perform a DPIA only where the processing operation is 'likely to result in a high risk to the rights and freedoms of natural persons'. See also, Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6, 2019, 105342, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2019.105342. (https://www.sciencedirect.com/science/article/pii/S0267364918304357)

44 ICO, note 6.

45 Tietosuojavaltuutetun toimisto, Case 531/161/20 1 (16), available at https://tietosuoja.fi/documents/6927448/22406974/Ty%C3%B6ntekij%C3%B6iden+sijaintitietojen+k%C3%A4sittely+ja+vaikutustenarviointi.pdf/2d04e545-d427-8a0d-3f4d-967de7b428ac/Ty%C3%B6ntekij%C3%B6iden+sijaintitietojen+k%C3%A4sittely+ja+vaikutustenarviointi.pdf.

46 EDPB, note 6, p. 7-8.

47 Tietosuojavaltuutetun toimisto, Diary number: 1150/161/2021 of December 7, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211183.

48 EDPB, note 6, p. 8-9.

49 Garante, Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. — 10 giugno 2021 [9685922], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685922.

50 EDPB, note 6, p. 9.

51 EDPB, note 6, p. 9-10.

52 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", WP 248 rev.01, 4 October 2017, available at ec.europa.eu/newsroom/document.cfm?doc_id=47711 (endorsed by the EDPB).

53 UODO, DKN.5101.25.2020 of November 12, 2020, available at https://uodo.gov.pl/decyzje/DKN.5101.25.2020.

54 See Article 4(5) GDPR for a definition of 'pseudonymization'.

55 EDPB, Guidelines 4/2019, p. 6, note 6. See also ENISA, 'Privacy and Data Protection by Design — from privacy to engineering', 2014, available at <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design >.

56 AEPD, 2019, note 6.

57 EDPB, note 6, p. 6.

58 L JASMONTAITE et al, note 2.

59 EDPB, note 6, p. 6.

60 APDCAT, note 6.

61 UODO, DKN.5130.2559.2020 of December 9, 2021, available at https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020%20.

62 UODO, ZSPR. 421.2.2019 of September 10, 2019, available at https://uodo.gov.pl/decyzje/ZSPR.421.2.2019.

63 ENISA, Guidelines for SMEs on the security of personal data processing of January 27, 2017, available at https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

64 Judgment of the Provincial Administrative Court in Warsaw, II SA/Wa 2559/19 of September 3, 2020 available at https://orzeczenia.nsa.gov.pl/doc/2F881CED73.

65 UODO, DKN.5131.22.2021 of July 13 2021, available at https://www.uodo.gov.pl/decyzje/DKN.5131.22.2021.

66 Hungarian National Authority for Data Protection and Freedom of Information, Case NAIH/2019/769/ (NAI-H/2018/5997/H.) of October 15, 2019, available at https://www.naih.hu/files/NAIH-2019-769-hatarozat.pdf.

67 L BYGRAVE, note 4, p. 116.

68 L JASMONTAITE et al, note 2.

69 EDPB, note 6, p. 10.

70 Tietosuojavaltuutetun toimisto, Diary number 6097/161/21 of May 9, 2022, available at https://finlex.fi/fi/viranomaiset/tsv/2022/20221483. See also the press release, available at https://tietosuoja.fi/-/otavamedial-le-seuraamusmaksu-puutteista-tietosuojaoikeuksien-toteutuksessa.

71 EDPB, note 6, p. 6-7. The EDPB further explains that quantitative metrics may be the level of risk, the reduction of complaints, the reduction of response time when data subjects exercise their rights and qualitative metrics can be evaluations of performance, use of grading scales, or expert assessments.

72 Irish DPC, Reference: IN-21-4-2 in the matter of Meta Platforms Ireland Ltd. (Formerly Facebook Ireland Ltd.) of November 25, 2022, available at https://www.dataprotection.ie/sites/default/files/uploads/2022-12/Final%20Decision_IN-21-4-2_Redacted.pdf. See also the press release, available at https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

73 A technique to limit network traffic to prevent users from exhausting system resources, which makes it harder for malicious actors to overburden the system and cause attacks like Denial of Service (DoS). See A EL KAMEL et al , 'On-the-fly (D)DoS attack mitigation in SDN using Deep Neural Network-based rate limiting' [2022]182 Computer Communications <https://doi.org/10.1016/j.comcom.2021.11.003 >.

74 UODO, DKN.5130.2815.2020 of January 11, 20210, available at https://www.uodo.gov.pl/decyzje/DKN.5130.2815.2020. With a similar subject-matter, rationale, and corrective actions, see **Cases PL9** and **PL10** (with references in Annex I of the Report).

75 See **Case PL-CR-1** with reference in Annex I of the Report.

76 EDPB, note 6, p. 6-7.

77 Garante, Provvedimento del 25 febbraio 2021 [9556958], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958 .

78 ANSPDCP, case of August 4, 2020, the press release is available at https://www.dataprotection.ro/?page=Comunicat_Presa_01_09_2020&lang=ro.

79 C DE TERWANGNE, *The EU General Data Protection Regulation (GDPR) – A Commentary*, 1st edn, Oxford University Press, 2020, p. 314.

80 EDPB, note 6, para 68.

81 Garante, Ordinanza ingiunzione nei confronti di Iliad Italia S.p.A. — 9 luglio 2020 [9435807], available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435807.

82 APD/GBA Numéro de dossier: DOS-2020-03432, Case: 85/2022 of May 25, 2022, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-85-2022.pdf.

83 PersónuVernd, Case no. 2020092451 of January 12, 2022, available at https://www.personuvernd.is/urlausnir/vinnsla-landsbankans-a-personuupplysingum-ekki-i-samraemi-vid-log.

84 Garante, Prescriptive and sanctioning measure against Ediscom SpA — 23 February 2023 [9870014], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014

85 Tietosuojavaltuutetun toimisto, Diary number 1509/452/18 of December 30, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211503.

86 Garante, Ordinanza ingiunzione nei confronti di Azienda sanitaria universitaria Friuli Centrale — 26 maggio 2022 [9790365], availabe at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9790365.

87 Garante, Linee guida in materia di dossier sanitario, June 4, 2015, available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4091542.

88 APD/GBA, note 52.

89 Tietosuojavaltuutetun toimisto, Diary number: 2368/182/20 of August 6, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211004 .

90 Irish DPC, decision of September 14, 2022, available at https://www.dataprotection.ie/sites/default/files/uploads/2023-01/Airbnb%20Ireland%20UC%20IN-21-3-1%20Redacted%20Decision%20EN.pdf.

91 AEPD Procedimiento Nº: PS/00003/2021 of February 25, 2022, available at https://www.aepd.es/es/documento/ps-00003-2021.pdf

92 Recital 39 GDPR.

93 Tietosuojavaltuutetun toimisto, Diary number 8493/161/21 of December 16, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211303

94 EDPB, note 6, para. 70.

95 Datatilsynet, Ref No 20/03087-14 of August 7, 2020, available at https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf.

96 Recital 50 GDPR. However, organizations do not need to rely on the Article 6(4) GDPR compatibility test in three circumstances: when they process data for archiving, scientific, or historical research purposes, as there is a presumption of compatibility under Article 5(1)(b); when they collect the individual's consent for the new processing purpose; or when the latter is based on a GDPR restriction under Article 23(1) GDPR.

97 EDPB, note 6, para 72.

98 APD/GBA, N° de dossier : DOS-2019-02974, Case: 53/2020 of September 1, 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-53-2020.pdf.

99 Cour d' appel Bruxelles, Case: 2020/AR/1333 of January 27, 2021, available at https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-27-januari-2021-van-het-marktenhof-ar-1333-beschibaar-in-het-frans.pdf.

100 Recital 39 GDPR.

101 EDPB, note 6, para 76.

102 ANSPDCP, case of June 27, 2019, available at https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro .

103 Tietosuojavaltuutetun toimisto, Diary number: 137/161/2020 of May 18, 2020, available at https://finlex.fi/fi/viranomaiset/tsv/2020/20200583.

104 Garante, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. — 22 luglio 2021 [9685994] available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994. The facts regarding the configuration of systems used by Deliveroo and the DPA's rationale are almost the same as the ones found in the earlier **Case IT13** concerning another food delivery company, Foodinho (referenced in Annex I of the Report). For an analysis of both cases from the perspective of the lawfulness of rider-management decisions undertaken by the companies under the GDPR, see S BARROS VALE and G ZANFIR-FORTUNA, Automated Decision-Making Under the GDPR — A Comprehensive Case Law Analysis, May 2022, available at https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpracomprehensive-case-law-analysis/

105 EDPB, Guidelines 3/2019 on processing of personal data through video devices, adopted on January 29, 2020, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

106 APD/GBA, Numéro de dossier : DOS-2019-04412, Case: 74/2020 of November 24, 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-74-2020.pdf.

107 AEPD, Procedimiento Nº: PS/00120/2021 of July 26, 2021 available at https://www.aepd.es/es/documento/ps-00120-2021.pdf. You can consult a more detailed summary of the case in S BARROS VALE and G ZANFIR-FORTUNA, note 118 , p. 43.

108 Munich Higher Regional Court, final judgment of December 8, 2020 – 18 U 2822/19, available at https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2020-N-34203.

109 Bundesgerichtshof, Judgement of January 27, 2022 — III ZR 3/21.

110 EDPB, note 6, para 79.

111 Irish DPC, DPC Case Reference: IN-19-7-2 of March 23, 2021, available at https://www.dataprotection.ie/sites/default/files/uploads/2021-05/Redacted_23.03.2021_Decision_IN-19-7-2.pdf.

112 The DPC's decision directly quotes and is inspired by the CJEU's Huber ruling, in which the CJEU held that "it is incumbent on the authority responsible for a register (...) to ensure that the data which are stored are, where appropriate, brought up to date so that, first, they reflect the actual situation of the data subjects and, secondly, irrelevant data are removed from that register". See CJEU, Case C-524/06 Heinz Huber v Bundesrepublik Deutschland, December 16, 2008, ECLI:EU:C:2008:724, para. 60.

113 Tietosuojavaltuutetun toimisto, Diary number: 834/532/18 of November 9, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211225#OT2.

114 Parliamentary Ombudsman, Judgement EOAK/945/2016 of August 11, 2017, available at https://www.oikeusasiamies.fi/r/fi/ratkaisut/-/eoar/945/2016.

115 Tietosuojavaltuutetun toimisto, Diary number: 8211/161/19 of November 9, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211223.

116 Information Commissioner's Office, INV/0561/2021 of June 7, 2022, available at https://ico.org.uk/media/action-weve-taken/reprimands/4023124/bolton-at-home-reprimand.pdf.

117 Article 5(1)(e) and Recital 39 GDPR.

118 EDPB, note 6, para 82.

119 BinBDI, case 711.412.1 of November 5, 2019, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.

120 Datatilsynet, Ref No 18/04147-23/KBK of February 25, 2020, available at https://www.datatilsynet.no/contentassets/0c61777547e74a6e90ad4555a1728869/varsel-om-vedtak-om-palegg-og-overtredelsesgebyr_statens-vegvesen.pdf.

121 EDPB, note 6, para 85.

122 ANSPDCP, Case of November 16, 2022, the press release is available here https://www.dataprotection.ro/?page=Comunicat_Presa_16_11_2022&lang=ro.

123 Datatilsynet, Journal number: 2019-442-4365 of April 22, 2020, available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/apr/kolding-kommune-havde-ikke-truffet-passende-tekniske-og-organisatoriske-foranstaltninger.

124 Conseil d'État — 1ère — 4ème chambres réunies, no 428451 of November 25 2020, available at https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042570046?tab_selection=cetat&searchField=ALL&query=428451&searchType=ALL&juridiction=TRIBUNAL_CONFLIT&juridiction=CONSEIL_ETAT&juridiction=COURS_APPEL&juridiction=TRIBUNAL_ADMINISTATIF&sortValue=DATE_DESC&pageSize=10&page=1&tab_selection=cetat#cetat.

125 Decree No. 2018-1254 of December 26, 2018 relating to medical information departments, available at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037864547/2020-12-08/.

126 APD/GBA, Dossiernummer: DOS-2019-05244, Case: 127/2022 of August 19, 2022, available at https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-127-2022.pdf. The facts and the decision of the Belgian DPA in this case are similar to the ones in **Case IT14** (referenced in Annex I of the Report), handled by the Italian Garante. On the other hand, the Austrian DPA seems less prone to act before the occurrence of a data breach. In **Case AT2** (also referenced in Annex I of the Report), after a complaint from an individual who was worried that a controller did not implement enough TOMs to prevent the leakage of personal data it was holding about them, the Austrian DPA noted that no data breach had yet occurred and thus the DPA could not act against the controller. The Austrian DPA added that, when it comes to TOMs, they "only create an obligation on the part of the data controller but not subjective legal claims of a data subject", meaning that there is no individual right for specific TOMs.

127 PersónuVernd, Case no. 2020010428 of March 10, 2020, available at https://www.personuvernd.is/urlausnir/oryggisbrestur-hja-saa-sektarakvordun .

128 **Case PL11** with reference in Annex I of the Report.

129 PersónuVernd, Case of March 10, 2020 available at https://www.personuvernd.is/urlausnir/nr/2885%20.

130 Supreme Administrative Court of the Republic of Bulgaria — Fifth Division, case No. 6307/27.06.2022 of June 27, 2022, available at https://info-adc.justice.bg/courts/portal/edis.nsf/e_act.xsp?id=1941175&code=vas.

131 Tietosuojavaltuutetun toimisto, Diary number: 4282/161/21 of December 16, 2021, available at https://finlex.fi/fi/viranomaiset/tsv/2021/20211244. The facts and the decision of the Finnish DPA in this case are similar to the ones in **Case IT15** (referenced in Annex I of the Report), handled by the Italian Garante.

132 APD/GBA Numéro de dossier : DOS-2020-04002, Case: 21/2022 of February 2, 2022, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf. See also the press release, available at https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr.

133 R Van EIJK, *Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden),* Amsterdam: Ipskamp Printing, ISBN 978 94 028 1323 4, 2019, available at https://ssrn.com/abstract=3319284.

134 PersónuVernd, Case no. 2020010656 of May 3, 2022 available at https://www.personuvernd.is/urlausnir/vinnsla-barnaverndarnefndar-hafnarfjardar-a-personuupplysingum-ekki-i-samraemi-vid-log.

135 UODO, DKN.5112.1.2020 of December 3, 2020, available at https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020.

136 EDPB, note 6, paras 64, 86, and 87.

137 Garante, Ordinanza ingiunzione nei confronti di Enel Energia S.p.a. — 16 dicembre 2021 [9735672], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9735672\.

138 AEPD Procedimiento Nº: PS/00236/2020 — May 4, 2021, available at https://www.aepd.es/es/documento/ps-00236-2020.pdf. See also the EDPB press release, available at https://edpb.europa.eu/news/national-news/2021/spanish-dpa-imposes-fine-1500000-euros-epd-energia-sau-two-infractions-gdpr_en.

139 Datenschutzbehörde, Case DSB-D123.822/0005-DSB/2019 of July 23, 2019, available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20190723_DSB_D123_822_0005_DSB_2019_00/DSBT_20190723_DSB_D123_822_0005_DSB_2019_00.html

140 Hungarian National Authority for Data Protection and Freedom of Information, Case No. NAIH/2020/2204/8 Cipőkereskedelmi Korlátolt Felelősségű Társaságnak Deichmann, issued September 3, 2020, available at https://www.naih.hu/files/NAIH-2020-2204-8-hatarozat.pdf.

141 Hungarian National Authority for Data Protection and Freedom of Information, Case No. NAIH-85- 3/2022 Budapest Bank, issued February 8, 2022, available at https://naih.hu//hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei.

142 EDPB, note 6, p. 11.

143 EDPB, note 6, p. 11-12.

144 EDPB, note 6, p. 12.

145 Tietosuojavaltuutetun toimisto, Diary number: 6813/171/21 of May 31, 2022, available at https://finlex.fi/fi/viranomaiset/tsv/2022/20221463.

146 PersónuVernd, Case no. 2021040879 of December 20, 2021, , available at https://www.personuvernd.is/urlausnir/akvordun-um-notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur.

147 EDPB, note 6, p. 12 and 13.

148 EDPB Guidelines 4/2019 p. 13-14, note 6.

149 Irish DPC, note 87.

150 Tietosuojavaltuutetun toimisto, Diary number:2984/182/2019 of June 26, 2020, available at https://finlex.fi/fi/viranomaiset/tsv/2020/20200601.

151 Joined Cases WM (C-37/20), Sovim SA (C-601/20), Grand Chamber, November 22, 2022, ECLI:EU:C:2022:912.

152 EDPB, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, adopted on February 14, 2023, available at https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

153 CNIL, Délibération SAN-2022-020 of November 17, 2022, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046562676.

154 N NOLTE und C WERKMEISTER, Art. 25 DSGVO in P Gola und D Heckmann (eds.), DSGVO/BDSG (3rd edn., C.H. Beck 2022).

155 LG Heilbronn, Bu 8 O 131/22, January 13, 2023, available at https://beck-online.beck.de/Dokument?vpath=bibdata%2Fents%2Fbeckrs%2F2023%2Fcont%2Fbeckrs.2023.330.htm&anchor=Y-300-Z-BECKRS-B-2023-N-330.

156 LG Stuttgart, Case No 53 O 95/22 of January 26, 2023, available at https://lnkd.in/euqZrMTS .

157 S BARROS VALE, *Upcoming Data Protection Rulings in the EU: An Overview of CJEU Pending Cases*, Future of Privacy Forum, September 15, 2021, available at https://fpf.org/blog/upcoming-data-protection-rulings-in-the-eu-an-overview-of-cjeu-pending-cases/.

158 Opinion of Advocate General Campos Sánchez-Bordona, Case C-300/21 UI v Österreichische Post AG, October 6, 2022, ECLI:EU:C:2022:756.

159 Opinion of Advocate General Giovanni Pitruzzella, Case C-340/21, VB against Natsionalna agentsia za prihodite, April 27, 2023, ECLI:EU:C:2023:353

160 HDPA, case 31/2019 of October 7, 2019, available at https://www.dpa.gr/sites/default/files/2019-12/31_2019anonym%20%281%29.pdf.

161 We note, however, that our research did not encompass decisions issued by DPAs solely on the basis of the national laws which transpose the ePrivacy Directive. For an example, see Comissão Nacional de Proteção de Dados, DELIBERAÇÃO/2019/297, May 6, 2019, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121715.

162 Article 13 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201.

163 CJEU, Case C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH, November 25, 2021, ECLI:EU:C:2021:954.

164 Garante, Ordinanza ingiunzione nei confronti di La Prima S.r.l. — 16 settembre 2021 [9705632], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9705632.

165 Hungarian National Authority for Data Protection and Freedom of Information, case NAIH-924-10/2021 of June 18, 2021, available at https://www.naih.hu/hatarozatok-vegzesek?download=405:erintetti-jogok-biztositasanak-kotelezettsege-nem-ugyfel-erintettek-reszere.

166 APD/GBA, Numéro de dossier : DOS-2019-04798, Case: 047/2021 of January 20, 2021 available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-04-2021.pdf.

167 Garante, Ordinanza ingiunzione nei confronti di Wind Tre S.p.A. — 9 luglio 2020 [9435753], available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435753.

168 HDPA, Case 13/2021 of April 17, 2021, available at https://www.dpa.gr/sites/default/files/2021-04/13_2021anonym.pdf.

169 HDPA, Case 20/2021 of May 12, 2021, available at https://www.dpa.gr/sites/default/files/2021-05/20_2021anonym.pdf.

170 Garante, Ordinanza ingiunzione nei confronti di Vodafone — 12 novembre 2020 [9485681], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681.

171 The subject-matter of the case and the Garante's rationale are similar to the ones in **Case IT16** (referenced in Annex I of the Report).

172 ICO, note 45. In its draft guidance, the regulator explains that "PETs and anonymisation are separate but related concepts. Not all PETs result in effective anonymisation, and you can achieve anonymisation without using them. At the same time, PETs can play a role in anonymisation, depending on the circumstances. (...) However, the purpose of many PETs is to enhance privacy and protect the personal data you process, rather than to anonymise that data." The guidance note explains the merits of eight specific PETs under the light of the GDPR, notably: homomorphic encryption; secure multiparty computation; private set intersection; federated learning, trusted execution environments, zero-knowledge proofs, differential privacy, and synthetic data.

173 Article 29 Working Party, 2014, Opinion 05/2014 on Anonymisation Technique, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

174 Datatilsynet, May 5, 2021, available at https://www.datatilsynet.no/contentassets/27d554561ceb4e77ad22b-54fad5bfe0e/vedtak-om-overtredelsesgebyr-til-norges-idrettsforbund.pdf.

175 Datatilsynet, note 6.

176 EDPS, *Is the future of privacy synthetic?*, July 14, 2021, available at https://edps.europa.eu/press-publications/press-news/blog/future-privacy-synthetic_en.

177 O TENE and G ZANFIR-FORTUNA, *Chasing the Golden Goose: What is the path to effective anonymisation?,* PinG, 2017, available at https://doi.org/10.37307/j.2196-9817.2017.04.03.

178 Recitals 26, 28, and 29, and Article 4(5) GDPR.

179 This high threshold for anonymization under the GDPR also draws from earlier guidance from EU DPAs and the jurisprudence of the CJEU. See ARTICLE 29 DATA PROTECTION WORKING PARTY, note 50, and CJEU, Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland, October 19, 2016, ECLI:EU:C:2016:779.

180 APDCAT, note 6.

181 AEPD, *Encryption and Privacy III: Homomorphic encryption*, June 22, 2020, available at https://www.aepd.es/en/prensa-y-comunicacion/blog/encryption-privacy-iii-homomorphic-encryption.

182 AEPD, *Anonymisation and pseudonymisation (II): Differential privacy*, October 28, 2021, available at https://www.aepd.es/en/prensa-y-comunicacion/blog/anonymisation-and-pseudonymisation-ii-differential-privacy.

183 AEPD, *Privacy by Design: Secure Multiparty Computation: Additive Sharing of Secrets*, May 30, 2022, available at https://www.aepd.es/en/prensa-y-comunicacion/blog/privacy-by-design-secure-multi-part-computation-additive-sharing-secrets.

184 AEPD, *Encryption and Privacy IV: Zero-knowledge proofs*, November 4, 2020, available at https://www.aepd.es/en/prensa-y-comunicacion/blog/encryption-privacy-iv-zero-knowledge-proofs.

185 AEPD, *GDPR compliance of processings that embed Artificial Intelligence — An introduction*, February 2020, available at https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf, p. 37.

186 Conseil d'État, case 450163 of December 3, 2021, available at https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043261200

187 Belgian Administrative Court, case No 251.378, of 19 August, 2021, A. 234.221/XII-9119.

188 Dutch DPA, September 30, 2019, available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-stelt-geen-onderzoek-naar-opslag-medische-gegevens-cloud

189 HDPA, Case 04/2022 of January 27, 2022, available at https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf.

190 Garante, Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano — 16 settembre 2021 [9703988], availabe at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988.

191 EDPB, note 6, paras. 42, 44, and 49.

192 Datatilsynet, Journal number: 2020-432-0034 of January 26, 2021, available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen.

193 HDPA 50/2021 of November 16, 2021, available at https://www.dpa.gr/sites/default/files/2021-11/50_2021anonym.pdf.

194 Tietosuojavaltuutetun toimisto, note 99.

195 **RO4** with reference in Annex I of the Report.

196 Austrian Supreme Court, Case: 6Ob77/20x of November 25, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20201125_OGH0002_0060OB00077_20X0000_000.

197 Austrian Supreme Court, Case: 6Ob77/20x of November 25, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20201125_OGH0002_0060OB00077_20X0000_000.

198 CJEU, Case C-319/20 Meta Platforms Ireland Limited, April 28, 2022, ECLI:EU:C:2022:322.

199 [HmbBfDI (Hamburg), J3, January 5, 2022, available at https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf.

200 Garante, Provvedimento del 25 marzo 2021 [9574709], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9574709.

201 Nonetheless, other DPAs have developed considerable efforts to advise controllers on how to implement age verification mechanisms that align with DPbD&bD, something that is also in the EDPB's most recent Work Program (note 44). In this regard, see Irish DPC, *Fundamentals for a Child-Oriented Approach to Data Processing*, December 2021, available at https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; and CNIL, *Online Age Verification: Balancing Privacy and the Protection of Minors,* September 22, 2022, available at https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

202 BYGRAVE, note 20.

203 See **Case PL5** and **Case IE2** as relevant examples.

204 ICO, Findings from the ICO's consensual audits on 11 multi academy trusts, September 2018 to October 2019, available at https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618610/mats-outcome-report-v1_1.pdf.

NOTES

The Future of Privacy Forum (FPF) is a global non-profit organization that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data use, identify the risks, and develop appropriate protections. FPF has offices in Washington D.C., Brussels, Singapore, and Tel Aviv.

FPF.ORG | FPF.ORG/EU | INFO@FPF.ORG

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005

AVENUE MARNIX 13-17 | 1000 BRUSSELS, BELGIUM