UNIO - *EU Law Journal*. Vol. 11, No. 2, October 2025, pp. 120-145.
®2025 Centre of Studies in European Union Law
School of Law – University of Minho

Harmonising privacy: the protection of personal data and digital rights in the European Union. Legal, political and technical barriers to a unified digital privacy framework across EU Member States

Luis Maurin Hakala*

ABSTRACT: This paper analyses the fragmented protection of individuals' personal data in the European Union, arguing that the General Data Protection Regulation (GDPR), while comprehensive in scope, falls short of ensuring uniform enforcement across Member States. Moreover, a theoretical framework around the evolving notion of personal data proves how combinations of anonymised information can re-identify individuals, challenging the GDPR's current definitional limits. This study thereby situates the GDPR within the broader, interdependent EU data governance framework, revealing overlaps and inconsistencies that undermine harmonisation. Using comparative case studies of Ireland, Spain, Italy, and Latvia, this paper demonstrates that enforcement diverges significantly across Member States due to differing institutional capacities, political wills, and administrative traditions. Applying theories of policy implementation and multi-level governance, it argues that EU-level law is weakened by practical differentiation. This analysis coincides with the European Commission's 2025 Digital Omnibus proposals, which aim to overhaul GDPR procedures and underscore the structural challenges examined in this paper.

KEYWORDS: Data protection – digital rights – GDPR – harmonisation – multi-level governance.

* Barcelona Center for European Studies (BACES), Universitat Pompeu Fabra, Barcelona, Spain.

1. Introduction

As long as a smart device is nearby, nearly every facet of human life can be subject to surveillance. Smart devices, used for a variety of purposes, generate data about individuals' behaviour, preferences, location, interests, habits and even emotions. This data is collected, processed and analysed to enable social media platforms to create highly detailed user profiles, which in turn are used to influence users' online behaviour. Within this business model, the aims of all online activity culminate in a transaction – user profiling is used to micro-target content, leading to increased engagement and personalised advertising strategies aimed at profit maximisation.[1]

In May 2018, the European Union (EU) implemented the General Data Protection Regulation [Regulation (EU) 2016/679] (GDPR), establishing one of the most comprehensive legal frameworks for personal data protection worldwide. The GDPR adopts a principles-based approach, focusing on empowering individuals with rights over their personal data while holding organisations accountable for its proper use. It grants individuals key rights such as access, rectification and the right to be forgotten, enabling them to control how some of their personal data is processed. Organisations are subject to strict standards, including obtaining valid consent, ensuring data minimisation and implementing robust security measures. Non-compliance can result in substantial penalties.[2]

Such legislation is imperative since, if data is for sale, then virtually every single aspect of individuals' lives can be converted into a tool to predict, track and manipulate thoughts, habits and personalities. This data "*(...) is in reality, our hopes and fears, our medical history, our most private conversations, our friends, our darkest regrets, our traumas, our joys*", in the words of author Carissa Veliz.[3]

Within this context, only internationally binding data protection law, such as the GDPR, can ensure consistent standards across all Member States. In a common digital market with a free flow of data, harmonised international law is most effective as digital companies and social media operate and move data worldwide. In other words, consistency can foster trust and safeguard individuals' rights within the single market, where the free movement of people, goods and services is a fundamental principle. By harmonising data protection rules, the GDPR is said to allow the seamless flow of personal data across borders while ensuring privacy and accountability within the context of ongoing European integration.[4] However, the protection of individuals' data is fragmented across various EU legislative acts, often causing uncertainty and inconsistencies that undermine the envisaged holistic approach to privacy and data security. For this reason, the GDPR alone is not as protective of data as needed in today's digital context.

---

[1] Sha Zhao, Shijian Li, Julian Ramos, Zhiling Luo, Ziwen Jiang, Anind K. Dey, and Gang Pan, "User profiling from their use of smartphone applications: a survey." *Pervasive and Mobile Computing* 59 (2019), https://doi.org/10.1016/j.pmcj.2019.101052; Imdad Ullah, Roksana Boreli, and Salil S. Kanhere, "Privacy in targeted advertising: a survey." *arXiv* preprint, 2021, https://arxiv.org/pdf/2009.06861.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Carissa Véliz, *Privacy is power: why and how you should take back control of your data* (New York: Melville House, 2020), 151.

[4] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler (ed.), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford: Oxford University Press, 2020).

Although the GDPR restricts user profiling, it allows exceptions, such as for contractual necessity, legal obligations or when there is explicit consent.[5] Nonetheless, this consent is often a condition for accessing major social media platforms, raising concerns about its voluntariness in a world ever more reliant on these platforms for cultural, economic, political and social participation. Amid this dependency on social media that engages in mass personal data collection, a complicated legal landscape creates practical challenges for both users and other stakeholders in navigating compliance and enforcement. This holds true especially for individuals who may want to invoke their own rights.

Moreover, it is unclear to what extent data subjects must be provided with individual explanations for the profiling activities. Personal data is not a straightforward concept and as technologies advance – such as reversing anonymisation – individuals are increasingly reidentified from datasets previously deemed anonymous.[6] This further narrows the distinction between personal and non-personal data.

As with any regulation within the EU, this kind of binding piece of legislation is applied in its entirety across the EU after being passed. However, the enforcement of its provisions falls largely under the responsibility of each Member State through their data protection authorities (DPAs). Furthermore, each Member State can opt to go beyond the GDPR's mandatory provisions and complement their application with more ambitious protections. These differences in scope, ambition and enforcement between Member States can signal the potential shortcomings of EU law – creating inequalities in individuals' data protection within the EU.

This analysis remains timely. The Commission's November 2025 Digital Omnibus package seeks to boost Europe's digital markets by easing constraints on data use, simplifying SME compliance, harmonising breach notifications, and resolving overlaps between several digital regulations and directives.[7]

Therefore, with the help of philosophical, legal, and governance components; this paper adopts a primarily policy-implementation lens to explain why the enforcement of the GDPR diverges across Member States. A conceptual discussion of personal data and anonymisation serves to clarify the scope of the legal object being implemented, revealing how ambiguity in defining *"personal data"* may condition every subsequent stage of governance. Later, these conceptual insights are linked to key institutional and political factors highlighted by EU legal scholarship and multi-level governance theory. Building on Hill and Hupe's (2002) policy-implementation framework and Börzel and Risse's (2003) "*goodness-of-fit*" logic, the paper shows how the GDPR regime produces differentiated national outcomes when conceptual uncertainty, administrative capacity, regulatory traditions, and political priorities interact.

[5] Regulation (EU) 2016/679 (General Data Protection Regulation).

[6] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation", *International Data Privacy Law* 7, no. 2 (2017): 76–99, https://doi.org/10.1093/idpl/ipx005.

[7] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the Digital Legislative Framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 19 November 2025; Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on Artificial Intelligence (Digital Omnibus on AI), COM(2025) 836 final, 19 November 2025.

In summary, the contribution of this article to the critical analysis of the protection of personal data in the EU consists of the following: (1) the provision of a profound insight into what personal data truly encompasses; (2) a diagnosis of the current holistic approach to data protection as ineffectively fragmented into numerous legislative acts; (3) the illustration of the different GDPR enforcement levels of Member States; (4) drawing on theories of policy implementation which highlight how enforcement processes in each Member State are shaped by domestic institutional and political factors.

As such, research questions (RQs) guiding this study are:

RQs: How does the implementation of the GDPR become differentiated across Member States, and why do such differences in enforcement emerge?

The article will attempt to depict the current state of the art in personal data protection by exploring these deficiencies. Section 2 will outline the historical context of European data protection law to better understand the present. Section 3 takes insights from the philosophy of communication to prove that the GDPR does not exhaust the scope of what can be understood as *"personal data."* Section 4 presents a description of the fragmentation in the current approach to data protection. Section 5 examines the factors that explain variation in GDPR enforcement across Member States. Section 6 then develops case studies to illustrate how these differences emerge in practice, highlighting the domestic challenges of transposing and enforcing the Regulation. Finally, the differences in GDPR enforcement by Member States are summarised and discussed in Section 7.

2. From the early internet, to data collection, to artificial intelligence

It is a truth universally acknowledged that life in the digital world must be governed by the same values endorsed in life without the internet or technological devices. The norms and beliefs that are upheld in offline behaviour in the physical world must also apply when interacting online. In parallel, when it comes to the right to exist online privately and independently, policymaking naturally revolves around the question of how to find a balance between the protection of individuals and commercial interests.

Directive 95/46/EC (the Data Protection Directive) – later replaced by the GDPR – was the EU's first significant piece of legislation on internet data protection, designed for an internet primarily used by academics, researchers and businesses, with limited public access. It extended basic privacy norms to the online world, emphasising fair data processing and individual consent. However, it lacked provisions for sensitive data, allowed inconsistent implementation across Member States and offered no unified penalties or strong supervisory authorities; reflecting the nascent state of digital technology at the time.[8]

The creation of the personal computer had been led in great part by Stewart Brand and Steve Jobs' intention to associate it with the quest for individual freedom. This personal computer would be free from corporate power and act as the authentic voice of its owner – a fruit of the desire for liberty and unconstrained expressiveness.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union, L 281, 23 November 1995, 31.

This gave birth to a cyberspace of the most autonomous and liberating sort. Later, the eventual launch of the smartphone in the first decade of the century would put computers into the pockets of hundreds of millions of individuals and provide an easy way to surf the World Wide Web anywhere and at any moment.[9] Ubiquitous access to the internet turned into mass usage, which then turned into mass data about its users.

Since the Lisbon Treaty of 2009, the EU has had explicit authority, under Article 16 of the Treaty on the Functioning of the European Union, to legislate on personal data protection and that data's free movement.[10] European legislation has attempted to keep pace with the risks and challenges of new technologies in order to regulate the expanding use of personal information in digital markets. However, early laws could not anticipate challenges like social media privacy, targeted advertising, or large-scale data-collection practices.

Not only is user data now stored, but so is metadata – such as IP (Internet Protocol) addresses, biometric and location data, and online activity – often collected through cookies and tracking technologies. The current business model of the internet therefore relies on turning online sessions into transactions, with platforms monetising user engagement through data-driven ads.[11] Social media, search engines and content platforms collect user data to deliver targeted ads, thereby generating profit without direct sales.

Consequently, online platforms compete for attention to drive engagement. The longer a user is kept on a platform, the more likely they are to be exposed to advertising. In an attention-based economy that is reliant on ad monetisation, platforms monitor and model user behaviour to predict actions, using profiling to deliver personalised content and nudges. Personalised ads are auctioned to the highest bidder, with businesses vying to reach ideal customers.[12]

3. The nature of personal data

According to Article 4 of the GDPR: *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*[13]

Therefore, personal information is defined as any information *"relating to"* an identified or identifiable natural person. An identifiable natural person is one who can be directly or indirectly identified, particularly through reference to specific identifiers. This could include information like a name, ID number, location data or anything else that can be linked back to that person. On the other hand, non-

[9] Gary Gerstle, *The rise and fall of the neoliberal order: America and the world in the free market era* (Oxford: Oxford University Press, 2022).

[10] Consolidated version of the Treaty on the Functioning of the European Union. Official Journal of the European Union, C 326, 26 October 2012, 47.

[11] Helen Nissenbaum, *Privacy in context: technology, policy, and the integrity of social life* (Stanford, CA: Stanford Law Books, 2010).

[12] Shoshana Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (New York: PublicAffairs, 2019).

[13] European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Regulation).*

personal data is electronic information that is either the product of personal data that has been anonymised or that in no way comes from a natural person (such as weather data). However, several scholars point to the under-theorisation of the notion of personal information. The possibility of de-anonymisation makes it unclear at what point personal information becomes non-personal information. Furthermore, as new technologies increasingly facilitate de-anonymisation, this distinction may become contingent or volatile. This leads some to assert that all data associated with individuals – even when anonymised – can ultimately qualify as personal data.[14]

The argument is that regulating only information or data that *"relates to"* a user is too restrictive. Instead, the GDPR presents a distinction between information that is directly about a person on its own, like a reference to their name or phone number, and other information that only becomes about a person when combined with additional details, like information about a friend. This invokes the notion of *"aboutness"*, a philosophy of language approach to infer that information that does not initially relate to an individual can still be about them when combined with other pieces of information. In other words, even data on a person's interconnected network (such as family members or an IP address) can generate data directly about them. For instance, the statement *"Sally is pregnant"* is not about John on its own, but when combined with *"Sally's father is John"*, it forms the new statement *"John's daughter is pregnant"*, which is absolute information about John.[15] The conjunction of these pieces of information constructs personal data about new users. Data regulation must therefore consider and act according to this complexity in the era of mass data collection, where complex combinations of data can reveal almost anything about a data subject. Combinations of anonymised or non-personal data can also yield personal data.

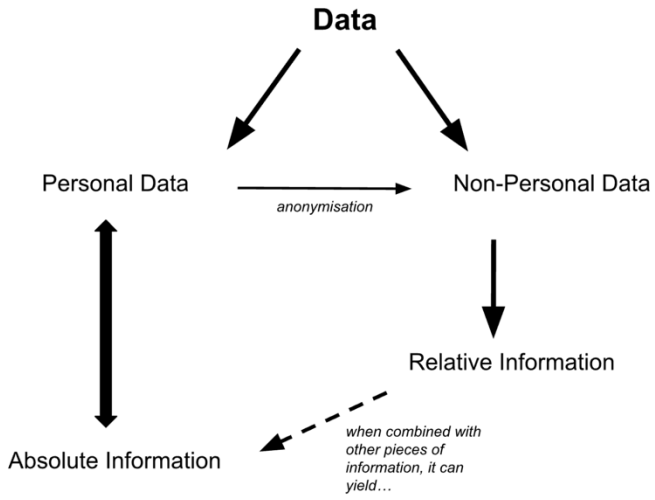

Figure 1: The Fluid Boundaries of Personal and Non-Personal Data

Even though the GDPR's definition of personal data is broad, its coverage of any situation in which data could reasonably be combined to identify a person makes enforcement challenging, given the inherent uncertainty of how data combinations

[14] Sille Obelitz Søe, Rikke Frank Jørgensen, and Jens-Erik Mai, "What is the 'personal' in 'personal information'?", Ethics and Information Technology 23, no. 4 (2021): 625-633, https://doi.org/10.1007/s10676-021-09600-3.

[15] Nelson Goodman, "I.-About", *Mind* 70, no. 277 (1961): 1-24, https://doi.org/10.1093/mind/LXX.277.1; Søe, Jørgensen and Mai, "what is the 'personal' in 'personal information'?", 629.

and re-identification risks evolve over time. External or anonymous data is covered only if it is anonymous at the moment of processing, and Recital 26 of the GDPR offers limited guidance on how re-identification risks change over time.[16] Therefore, information that might eventually yield lucrative personal data through combination and contextualisation may be collected beyond the Regulation's immediate scope.

These protections are essential as the Charter of Fundamental Rights of the European Union (hereinafter, the Charter) mentions and distinguishes between the rights to data protection and privacy. Article 8 of the Charter, *"Protection of personal data"*, specifically establishes data protection as a fundamental right, granting individuals the right to access their personal data and ensuring that it is processed fairly and lawfully. This includes the right to know what personal data is being collected, how it is being used, and to have access to it. Additionally, Article 8 states that personal data must be processed for specified purposes that are based on consent or legitimate means laid down by law. On the other hand, the right to privacy is a broader concept that encompasses the protection of individuals' personal and private lives. This includes the right to protection against the unauthorised processing of personal data, along with the right to protection against surveillance and other forms of interference in one's private life.[17]

If personal information is understood as data that generates meaning about someone, then datafication – the transformation of everyday activities into data – enables the creation of valuable personal profiles by combining multiple data points that were initially meaningless or anonymous.[18] This highlights the complex relationship between mass data collection and privacy due to the potential risks that the indiscriminate collection of supposedly anonymous data may pose to individual privacy.

3.1. The novel challenge of artificial intelligence

Artificial intelligence (AI) has further transformed data collection and processing, automating these tasks for companies. It is no surprise that businesses reliant on ad monetisation, such as Google and Meta, lead in AI innovation. The growing presence of AI in daily life introduces new sources of personal data and enables the large-scale automation of data processing to optimise ad timing, combining users' browsing histories, brand interactions and shopping cart activity to deliver more precisely targeted advertisements. Without proper legal protection, internet autonomy will become endangered and online life may become unprotected, tracked, manipulated, surveilled, and endlessly auctioned.[19]

Regulation (EU) 2024/1689 (the Artificial Intelligence Act), passed in 2024, emphasises transparency in AI training data, human oversight, and regulatory bodies. It contains risk-based obligations with detailed requirements, though some rely on

[16] Regulation (EU) 2016/679 (General Data Protection Regulation).

[17] European Parliament, Council of the European Union, and European Commission, Charter of Fundamental Rights of the European Union, 2012. Official Journal of the European Union, C 326, October 26, 2012, 391–407.

[18] Jens-Erik Mai, "Big data privacy: the datafication of personal information," *The Information Society* 32, no. 3 (2016): 192–199, https://doi.org/10.1080/01972243.2016.1153010.

[19] Huixin Zhong, Eamonn O'Neill, and Janina A. Hoffmann, "Regulating AI: applying insights from behavioural economics and psychology to the application of Article 5 of the EU AI Act", Centre for Doctoral Training in Accountable, Responsible and Transparent AI, University of Bath, 2024, https://doi.org/10.1609/aaai.v38i18.29977; Zuboff, *The age of surveillance capitalism.*

principles such as data quality.[20] This may leave national and EU courts to develop case law as the future scope and risks of AI remain uncertain.

4. The fragmented legal framework of personal data protection

The race to regulate these risks against high-speed advances calls for robust and predictive legislation. However, what is most important is for any EU law to be equally implemented in all Member States at a time when the social media field is defined by instant transplanetary connectivity. The jurisdiction responsible for the protection of data cannot realistically be limited to borders that are not obeyed by the flow of data.

Within the EU, the data market is rapidly growing with advancements driven by AI, machine learning and the need for data-driven insights in sectors like healthcare, finance and energy. While the EU leads in ambitious personal data protection, the overall markets' reliance on data underpins the role of free-flowing information as a cornerstone of the digital economy. The EU's holistic data governance approach attempts to balance openness and privacy, fostering a digital economy that respects individual rights. Post-GDPR legislation aims to boost competitiveness by addressing market inefficiencies in data circulation. However, this increased data flow often challenges the protection of the preceding definitions of personal data protection.[21] The balance between safeguarding individual rights and enabling economic benefits through data circulation is still evolving.

The data economy encompasses all gains from data exchange, use, skills and storage. In this sense, the intent of this paper is to analyse citizens' rights within the data market. For this reason, the focus on the GDPR as the cornerstone of data protection must not be eclipsed by the importance of complementary acts. The EU has developed a complex, interdependent framework of laws regarding the flow of data. These protections are best understood as a holistic whole, designed to safeguard individual rights.

First off, legislation adapted to modern-day data flow was gradually introduced through the European Union's digital single market (DSM) strategy – a 2015 initiative aimed at creating a seamless and integrated online market across all Member States. It seeks to remove digital barriers, foster innovation, and improve access to digital goods as well as services within the EU. Key initiatives, such as the e-commerce package, the Digital Education Action Plan and the European cloud initiative, have been introduced to make cross-border parcel delivery more affordable, boost digital skills and enhance cloud computing infrastructure, respectively. These endeavours highlighted the intention to foster efficient non-personal data sharing for the European digital economy. This strategy highlights the need to balance data protection with economic interests, supporting innovation and digital commerce through the DSM strategy. In other words, it seeks to unlock the full potential of the EU's digital sector, driving economic growth, job creation and competitiveness. In

[20] European Parliament and Council. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, L, July 12, 2024.

[21] European Parliament, Directorate-General for Internal Policies of the Union, *The emergence of non-personal data markets* (Luxembourg: Publications Office of the European Union, October 2023), https://data.europa.eu/doi/10.2861/781155.

parallel, sector-specific legislation, such as Regulation (EC) No 1907/2006 (requiring the sharing of chemical safety data), Directive (EU) 2015/2366 (on financial data sharing) and Regulation (EC) No 178/2002 (requiring public access to scientific data regarding new ingredient approvals), complements the digital legislation framework to address unique industry challenges.[22]

4.1. The General Data Protection Regulation

While the GDPR's formal definition in Article 4(1) establishes a low legal threshold for what qualifies as personal data – encompassing any information that could directly or indirectly identify an individual – it simultaneously excludes anonymised data from its scope, if deemed irreversible – thereby overlooking how such data can be recombined or cross-referenced to re-identify individuals and thus yield personal data once again.[23] Although this legal framework distinguishes personal from non-personal data, this boundary blurs as non-personal data can become personal when combined with other information. This complexity underscores the need for clear principles, rules and transparency in data processing.

The GDPR, effective from May 2018, establishes a comprehensive legal framework aimed at safeguarding personal data and protecting the privacy rights of individuals within the EU. It imposes strict obligations on organisations processing personal data, including obtaining explicit consent, minimising data collection, and implementing protective measures by design and by default. It grants individuals rights, such as access to their data, and requires organisations to adopt technical and organisational safeguards. Aligned with the EU's strategy to promote data collaboration and create a unified European digital market, the GDPR seeks to harmonise data protection laws, thus enabling the free flow of personal data across Member States.[24]

The GDPR established the European Data Protection Board (EDPB) to provide guidelines on data protection laws while national DPAs offer clear guidance to data controllers and subjects.[25] This ensures effective implementation and understanding of data protection practices among all stakeholders.

Specific GDPR articles directly address online personal data processing. The following are some of the most relevant articles concerning the protection of personal data:

- **Articles 1–3.** Affirm that the GDPR establishes rules on the protection of natural persons regarding the processing of personal data and on the free movement of such data. They apply to data processed in the EU by organisations both within and, in certain cases, outside the Union.
- **Article 5.** Delineates key personal data processing principles such as lawfulness, fairness, transparency and data minimisation.
- **Article 6.** Specifies legal bases required for processing personal data online, ensuring data is handled appropriately and legally.
- **Article 7.** Sets strict standards for obtaining valid consent online, requiring it to be freely given, specific, informed and unambiguous.

[22] European Parliament, Directorate-General for Internal Policies of the Union, *The emergence of non-personal data markets.*

[23] Søe, Jørgensen, and Mai, "What is the 'personal' in 'personal information'?", 629.

[24] Søe, Jørgensen, and Mai, "What is the 'personal' in 'personal information'?", 629.

[25] Article 29 Data Protection Working Party, "Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679", 13 February 2018, https://ec.europa.eu/newsroom/article29/items/611237.

- **Articles 12–15.** Ensure transparency in online data processing, requiring organisations to provide clear information about data collection and use and notify individuals when data is obtained from other sources, while also granting them access to their personal data.
- **Article 18.** Enables individuals to limit how their personal data is processed online.
- **Articles 21–22.** Grants the right to object to processing, particularly for direct marketing; and provides protection from decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects.
- **Articles 32–34.** Require data controllers and processors to implement security measures to protect personal data against unauthorised access, disclosure or loss, and to notify the supervisory authority and affected individuals in the event of a personal data breach.

4.2. Complementary initiatives

Building on the DSM strategy, the 2020 European strategy for data aims to create a single European data space, with a focus on promoting data-driven innovation and improving data sharing and reuse, while ensuring the protection of personal data and intellectual property rights. Focusing on the data economy as a whole, with a broader scope than the 2015 strategy, it highlights investments in infrastructure and technologies like AI and cybersecurity. It also proposes sector-specific data spaces for areas like healthcare and energy to drive sectoral innovation.[26]

In parallel, to develop a framework for data governance and sharing, Regulation (EU) 2022/868 (the Data Governance Act) was introduced to harmonise national regulations, promote voluntary data sharing and build trust among stakeholders through neutral data intermediaries, followed by a proposed data act to enhance access and reuse of data. Regulation (EU) 2023/2854 (the Data Act), in turn, proposes rules for data access, reuse and sharing. This includes provisions for data portability and data interoperability, seeking to promote fairness and competition in the data market. The created framework prevents unauthorised transfers of data to non-EU countries where privacy protections are insufficient and fosters a voluntary sharing of data among businesses, individuals and public sector bodies.[27]

However, challenges persist as transparency concerns arise with Directive (EU) 2016/943 (the trade secrets directive), which could limit data sharing due to concerns about the protection of trade secrets and confidential information, including measures to prevent unauthorised disclosure and use. Yet, the directive may need to be balanced with the need for transparency in data processing to ensure compliance with personal data protection. The trust in these frameworks relies heavily on active stakeholder engagement, which is crucial for their success and depends on adequate transparency measures.[28]

---

[26] European Commission, A European strategy for data, COM(2020) 66 final, 19 February 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[27] Gabriele Carovano and Michèle Finck, "Regulating data intermediaries: the impact of the Data Governance Act on the EU's data economy", *Computer Law & Security Review* 50 (2023), https://doi.org/10.1016/j.clsr.2023.105830.

[28] Daniele Arcidiacono, "The trade secrets directive in the international legal framework", *European Papers* 1, no. 3 (2016): 1073–1085, https://doi.org/10.15166/2499-8249/83.

Regulation (EU) 2018/1807 (the free flow of non-personal data regulation), initially enacted in 2018 to complement the GDPR but extended by the Data Governance Act, underscores the EU's commitment to seamless data integration across sectors, while maintaining stringent personal data protections and fostering an innovative data-driven economy. Its main objective is to remove unjustified data localisation restrictions imposed by Member States, allowing businesses and public authorities to store and process non-personal data anywhere in the EU. This regulation complements the GDPR by focusing on non-personal data, such as aggregated and anonymised datasets.[29]

Directive (EU) 2019/1024 (the open data directive) further complements the 2020 strategy. It fosters the reuse of public sector information, aligning with the GDPR by ensuring personal data protection during data sharing.[30] Moreover, Regulation (EU) 2022/1925 (the Digital Markets Act) targets anti-competitive practices among large digital platforms – referred to as gatekeepers – and intersects with data protection measures to ensure fair digital market competition. While its main focus is on curbing anti-competitive practices, the regulation includes provisions that intersect with the protection of individuals' personal data online.[31]

It is important to remark that the legal framework is still being built as of 2025. Directive 2002/58/EC (the ePrivacy directive) is expected to be replaced by the proposed ePrivacy regulation of 2017, which aims to update and harmonise privacy rules across the EU in line with technological advancements and the GDPR.[32] Known as the *"cookie law"*, it mandates informed consent for data collection practices, particularly with cookies, ensuring user control over personal data tracking.[33]

Furthermore, in November 2025, the European Commission published two major proposals – the Digital Omnibus and the Digital Omnibus on AI – and launched a Digital Fitness Check as part of a broader simplification agenda for EU digital regulation. In these packages, the Commission recognises regulatory fragmentation, divergent interpretations, and inconsistent DPA enforcement. They also address overlaps between the GDPR, ePrivacy Directive, Data Act, DGA, and DMA; proposes amendments aimed at simplifying compliance; and seeks to reduce administrative burdens.[34]

---

[29] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. Official Journal of the European Union, L 303, 28 November 2018, 59; Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union, L 152, June 3, 2022, 1.

[30] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. Official Journal of the European Union, L 172, 26 June 2019, 56.

[31] European Parliament and Council. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). Official Journal of the European Union, L 265, October 12, 2022, 1.

[32] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Council Document ST 6087/2021 INIT (e-Privacy Regulation Draft), 2021.

[33] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM(2017) 10 final, 10 January 2017.

[34] European Commission, Digital Omnibus, COM(2025) 837 final; European Commission, Digital Omnibus on AI, COM(2025) 836 final.

At the same time, the Digital Omnibus on AI Regulation weakens several oversight and transparency safeguards originally built into the AI Act in order to boost competitivity and innovation. Yet the European Investment Bank's own impact assessment notes that Europe's weak AI performance stems significantly from skills shortages, financing constraints, and national market fragmentation[35] – not regulation alone.

These packages remain proposals and may change during the legislative process. However, the most problematic element concerns a clarification of the scope of the definition of personal data, which introduces subjective, controller-specific identification tests. These developments may hamper enforcement and undermine data-subject rights. The Digital Omnibus would amend Article 4 GDPR by reinforcing the idea that information is not personal data for a given controller when that controller does not have means reasonably likely to identify the data subject.[36]

The proposal therefore shifts the GDPR's identification test from whether *anyone* could reasonably re-identify a person to whether the specific *controller in question* could do so, thereby narrowing the scope of what counts as personal data. This effectively further broadens the category of 'non-personal' data and risks placing additional pseudonymised data outside GDPR protection, even when other actors could re-identify individuals.

Other proposed changes include making data subjects' right of access conditional on demonstrating that the request is made for data-protection purposes or widening the exemption of organisations from keeping records of processing activities unless processing is risky, non-occasional, or involves special-category data.[37]

4.3. A fragmented chaos for the protected individuals

In conclusion, while the GDPR is central to the EU's data protection regime, the surrounding legal landscape – comprising various sector-specific laws and initiatives – illustrates the fragmented nature of data protection within the EU. This complexity may challenge the seamless protection intended by these frameworks, thus demanding ongoing evaluation and adaptation. Additionally, all directives require Member State transposition into national law, thereby further differentiating the practical implementation in each national jurisdiction. The cumulative effect of this fragmentation determines the level of protection that data subjects receive, depending on the Member State in which their rights are enforced.

In other words, in the quest to ensure competitiveness with a large array of legislative acts that attempt to stimulate the data economy, the EU's legal framework for the protection of personal data is challenged by individuals' difficulty to understand and refer to their rights in everyday life. The GDPR, as the magnum opus of digital rights, is complemented by other crucial acts that require significant Member State interpretation (both in transposition and enforcement). In a common data market, this decentralisation and weak procedural standardisation of individuals' basic rights may hinder the simplicity needed for effective enforcement.

[35] European Investment Bank, *Investment barriers in the European Union 2023: a report by the European Investment Bank Group* (Luxembourg: European Investment Bank, 2023).
[36] European Commission, Digital Omnibus, COM(2025) 837 final.
[37] European Commission, Digital Omnibus, COM(2025) 837 final.

5. Challenges in Member States: actors and institutions

This section examines the legal framework for personal data protection in the EU, aiming to analyse potential differences in the implementation of data protection in each Member State. This question gains importance since in a digital single market – where data flows freely – disparities in national regulations can expose individuals from highly protected jurisdictions to data protection risks in neighbouring countries.

The interaction between data markets, GDPR enforcement, and data protection challenges requires a multidimensional analysis to understand the factors driving variations in implementation. Legal, technological and economic factors largely determine the use and access of data within the data market. These are strongly interrelated and shaped by competing interests; the free flow of data and the protection of personal data.[38]

These factors must also be understood as incarnated by the interests and necessities of key stakeholders within the data market. The technological dimension of data sharing revolves around the extensive collection and profiling of individuals through online activities, primarily for micro-targeting. Personal data is collected, used, and sold to the highest bidder; driven by economic incentives.[39] This dynamic underscores the deep interdependence between technological advancements and economic forces, which in turn are defined by the actions of the businesses that exploit personal data. Lastly, the implementation of the legal framework in everyday life is subject to the circumstances of political processes – in which national lawmakers, lawyers, activists and civil society gain protagonism.[40]

In the business world, although transactions related to data between businesses often lack transparency, in theory they are limited by the current legislation's anonymisation requirements. Extensive research on anonymisation methods exists, but there is limited insight into their real-world application by practitioners, particularly beyond the scope of major tech companies. The temptation of businesses to apply legal requirements rather laxly may emerge, as anonymisation techniques can reduce the utility of the data and restrict its exploitability. Businesses seek to maximise the collection of minimally anonymised data.[41] These transactional dynamics are opaque and largely unknown.

On the other hand, difficulties in complying with legislation (notably the GDPR) present another significant barrier. Studies highlight that a significant portion of companies in Germany are hesitant to pursue innovations due to uncertainties surrounding the interpretation of GDPR requirements. Some businesses report avoiding the adoption of new technologies, such as those involving big data or AI,

[38] European Parliament, Directorate-General for Internal Policies, *The emergence of non-personal data markets.*

[39] Carovano and Finck, "Regulating data intermediaries."

[40] Laurie Robinson, "Europe's data privacy revolution: how civic engagement is impacting implementation", College of Information, University of Maryland, 31 March 2023, https://ischool.umd.edu/news/europes-data-privacy-revolution-how-civic-engagement-is-impacting-implementation/; Wojciech Wiewiórowski, "Civil society organisations as natural allies of the data protection authorities," *European Data Protection Supervisor*, 15 May 2018, https://www.edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_en.

[41] Alexandra Kapp, "Collection, usage and privacy of mobility data in the enterprise and public administrations", *Proceedings on Privacy Enhancing Technologies* 2022, no. 4 (2022): 440–456, https://doi.org/10.56553/popets-2022-0117.

while others face challenges in establishing data-sharing arrangements or creating collaborative data pools with partners.[42] Such lack of confidence reflects businesses' awareness of the risks and their fear of unintentionally failing to comply with data protection law.

Furthermore, the unequal presence of the largest data users in the EU is a remarkable factor. Major global multinational companies, including Facebook, Google, LinkedIn, Apple, PayPal and Airbnb, have all opted to base their European headquarters in Dublin.[43] This is notable because of the differing amounts of resources needed to control such presence at a time when Member States have differing degrees of practical implementation.

5.1. The role of politics

One explicative theory behind differing degrees of data protection implementation in Member States may be founded on the different weights of their respective political actors. For instance, the lack of strong advocacy and social awareness may significantly hinder the further application and pressure for the robust implementation of GDPR rules. Likewise, the absence of non-governmental organisations actively championing data protection rights can leave a critical gap in public advocacy and oversight, reducing the momentum needed to push for stricter enforcement.[44]

Additionally, the general lack of awareness among the public and smaller organisations about individual rights and obligations under GDPR further undermines the Regulation's effectiveness, as uninformed stakeholders are less likely to demand compliance or recognise violations. Moreover, when data protection issues are not a priority on political or organisational agendas, concrete actions and innovations to strengthen GDPR implementation stall, leaving its transformative potential unfulfilled.[45]

Civil society organisations (CSOs) are instrumental in advocating for robust data protection standards, educating the public about their rights, and holding both governments and corporations accountable for data privacy practices. Citizens can lack the knowledge to assess or advocate for their rights, compounded by limited education on data protection. By actively engaging in policy discussions, raising awareness and providing resources; CSOs ensure that data protection remains a central focus in the digital age, thereby empowering individuals to exercise their rights effectively.[46]

CSOs are therefore natural allies of data protection authorities, advocating for robust data protection standards and empowering individuals to assert their

[42] Alexandra Kapp, "Collection, usage and privacy of mobility data in the enterprise and public administrations", 440-456.

[43] Jenny Egnér Lin, "Facebook, Google, LinkedIn – why do all major tech companies place their European headquarters in Dublin?", *European Higher Education Fair*, 2019, https://ehef.id/post/facebook-google-linkedin-why-do-all-major-tech-companies-place-their-european-headquarters-dublin/en.

[44] Robinson, "Europe's data privacy revolution."

[45] Yelena Smirnova and Victoriano Travieso-Morales, "Understanding challenges of GDPR implementation in business enterprises: a systematic literature review", *International Journal of Law and Management* 66, no. 3 (2024): 326-344, https://doi.org/10.1108/IJLMA-08-2023-0170.

[46] Vera Franz, Ben Hayes, and Lucy Hannah, "Civil society organizations and General Data Protection Regulation compliance: challenges, opportunities, and best practices", *Open Society Foundations*, 7 February 2020, https://www.theengineroom.org/wp-content/uploads/2020/02/GDPR_Report-2019_12_16.pdf.

rights.[47] Without these efforts, there is a risk of under-enforcement of the GDPR in the Member States concerned; thereby jeopardising individual rights and hindering progress toward a fair digital landscape.

For instance, in France, CSOs played an active role in defending digital rights and privacy and raising awareness around these issues.[48] Such activity by civil society may have helped France to enact one of the most ambitious legal frameworks. The *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, as amended by the *Law No. 2018-493 on the Protection of Personal Data*, aligns with the GDPR and adds stricter sector-specific regulations – while granting enhanced powers to the National Data Protection Commission.[49] Similarly, in Spain, growing public debate and activism around privacy – particularly during the implementation of the GDPR – coincided with the adoption of the Ley Orgánica 3/2018, which not only transposed the Regulation but also expanded it by codifying new digital rights, such as the right to workplace disconnection and restrictions on political data use.[50]

On the contrary, the GDPR also permits Member States to introduce specific national provisions in certain areas, such as processing personal data for archiving purposes, scientific research, or statistical purposes. However, Member States such as Bulgaria, Hungary, Lithuania and Romania have chosen to not impose supplementary national rules in these areas beyond the GDPR's provisions.[51]

The political stability of a country is an additional important factor. A weak or otherwise divided government can struggle to implement novel and effective legislation due to trouble overcoming economic pressures.[52]

5.2. The role of institutions

Furthermore, the protection of digital rights in data handling may be complicated by legal and technological barriers. The technological capabilities of businesses determine their data analysis proficiency and the extent to which, for instance, they successfully anonymise the data they use. The GDPR provides limited concrete guidance on balancing data protection with economic and social interests. This ambiguity necessitates balancing competing interests; a challenge that may be heightened by the complexity and far-reaching impacts of AI and big data technologies.[53]

The GDPR established the EDPB to offer guidelines for interpreting and applying data protection laws, particularly in areas related to data reuse and open

[47] Wiewiórowski, "Civil society organisations as natural allies."

[48] Adrien Sénécat, "Algorithme de ciblage antifraude dans les CAF: Des associations saisissent le Conseil d'État", *Le Monde*, 16 October 2024, https://www.lemonde.fr/les-decodeurs/article/2024/10/16/algorithme-de-ciblage-antifraude-dans-les-caf-des-associations-saisissent-le-conseil-d-etat_6353442_4355770.html.

[49] International Comparative Legal Guides, "Data protection laws and regulations: France 2024-2025", 31 July 2024, https://iclg.com/practice-areas/data-protection-laws-and-regulations/france.

[50] Miguel Recio, "Spain's new data protection law: more than just GDPR implementation", International Association of Privacy Professionals (IAPP), 8 January 2019, https://iapp.org/news/a/spains-new-data-protection-law-more-than-just-gdpr-implementation.

[51] Detlev Gabel and Tim Hickman, "GDPR guide to national implementation", *White & Case*, 13 November 2019, https://www.whitecase.com/insight-our-thinking/gdpr-guide-national-implementation.

[52] Michael Hill and Peter Hupe, *Implementing public policy: governance in theory and in practice* (London: Sage, 2002).

[53] European Parliamentary Research Service, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, June 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

data initiatives. These guidelines aim to ensure compliance in Member States while promoting innovation and accessibility. Member States' DPAs are tasked with offering clear and practical guidance, especially when approached by data controllers seeking advice or responding to inquiries from data subjects. DPAs play a crucial role in ensuring that data protection practices are effectively implemented and understood by all stakeholders in the data economy.[54]

The GDPR also grants DPAs the power to enforce the law, including issuing fines for non-compliance. Fines are calculated to be effective, proportionate and dissuasive; with their severity determined by factors such as the nature, gravity and duration of the infringement. Nonetheless, the lack of institutional harmonisation among EU Member States risks personal data misuse, and current EU data-sharing measures are often fragmented. This results in overlaps and gaps that undermine legal clarity and accountability. The successful application of the GDPR's protection of personal data depends heavily on the extent to which non-compliance is appropriately sanctioned. Yet, DPAs offer differing degrees of data protection in each Member State despite a common data market.[55]

According to a 2024 report by the Commission on the application of the GDPR, many DPAs cite insufficient technical expertise, financial constraints and staff shortages as barriers to effective enforcement; particularly in handling high volumes of complaints.[56] Businesses also face increased administrative burdens and legal uncertainty, while individuals may experience weaker protections depending on the jurisdiction. This lack of uniformity creates compliance challenges for businesses operating across multiple jurisdictions and raises concerns about the unequal protection of data subjects' rights.

Additionally, procedural obstacles in various Member States, such as high thresholds for privacy violations and premature complaint dismissals, further hinder effective enforcement.[57] Weak procedural harmonisation, resource disparities among DPAs and diverging legal interpretations create systemic inefficiencies that weaken individuals' ability to exercise their rights and accountability for violations.

Reported cases of lack of coordination further exacerbate the issue. For instance, the Spanish data protection authority dismissed a citizen's complaint, stating that Ireland had jurisdiction over e-privacy violations since the company in question was headquartered there. However, the Irish authority refused to process e-privacy cases from non-residents. As a result, the Spanish data subject was unprotected against e-privacy violations by a company based in Ireland.[58]

The European Commission's 2024 report also criticises the regulation's one-stop-shop mechanism. Though the mechanism was designed to ensure consistent

[54] Orla Lynskey, "Complete and effective data protection", *Current Legal Problems* 76, no. 1 (2023): 297–344, https://doi.org/10.1093/clp/cuad009.

[55] Susan McGregor and Hugo Zylberberg, "Understanding the General Data Protection Regulation: a primer for global publishers", *Columbia Journalism Review*, 7 March 2018, https://www.cjr.org/tow_center_reports/understanding-general-data-protection-regulation.php.

[56] European Commission, Second report on the application of the General Data Protection Regulation (GDPR), COM(2024) 357 final, July 25, 2024.

[57] NOYB – European Center for Digital Rights. "5 years of the GDPR: national authorities let down European legislator", 23 May 2023, https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator.

[58] NOYB – European Center for Digital Rights. "Spain: key information", 2023, https://noyb.eu/sites/default/files/2023-05/DEF%20OnePager%20Spain.pdf.

enforcement across Member States by requiring cooperation among DPAs in cross-border cases, significant procedural differences and national interpretations of GDPR provisions continue to hinder its efficiency. While DPAs have increased cooperation through mutual assistance requests and informal consultations, the lack of binding obligations for response deadlines weakens enforcement efforts. Moreover, the EDPB plays a crucial role in resolving disputes, particularly on legal bases, such as data processing, transparency obligations, data breaches and administrative fines. This is important particularly as DPAs interpret key concepts differently, leading to legal fragmentation. However, dispute resolution procedures require significant time and resources, thereby potentially delaying remedies for some individuals and contributing to legal uncertainty in GDPR implementation.[59]

Analysing the frequency of sanctions imposed by DPAs and their amounts helps illustrate the asymmetrical enforcement of data protection. Figure 2 represents publicly disclosed fines, until March 2025, that refer to the GDPR articles that aim to protect personal data (mentioned in Section 4). These fines relate to Articles on insufficient fulfilment of data subjects' rights (12, 15, 17, and 21) and information obligations (5, 6, 7, 12, 13, 14, and 25), according to a GDPR Enforcement Tracker.

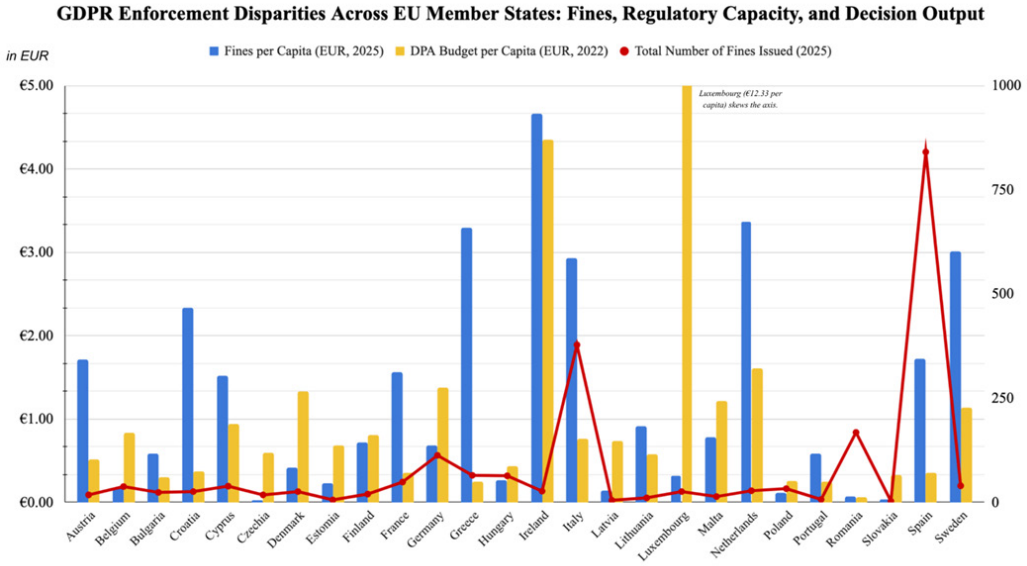

Figure 2: GDPR Enforcement Disparities Across EU Member States: Per-Capita Fines, DPA Budgets, and Total Decisions

NB: No information related to fines was found for Slovenia. *Sources:* The fine amounts were obtained from the GDPR Enforcement Tracker,[60] while the population data for 2024 was sourced from the Eurostat database.[61]

The methodology employed is simple. The total value of fines imposed by each Member State, as mentioned in Section 4, was divided by that Member State's respective population to calculate the sanctions issued per capita. To minimise distortions in the analysis, fines exceeding €50 million were excluded, such as the fine imposed by the Netherlands on Uber Technologies Inc. and the fines imposed

[59] European Commission, Second report on the application of the GDPR.
[60] CMS Law-Now, GDPR Enforcement Tracker, 2024, https://www.enforcementtracker.com/.
[61] Eurostat, "Population on 1 January 2024", https://ec.europa.eu/eurostat/databrowser/bookmark/7f401eba-93c4-4a9e-8a1d-22f2c943cb9b.

by Ireland on Meta Platforms,[62] which may also have a broader impact on all Europeans rather than just their own nationals. Meanwhile, DPA budget per capita was calculated by dividing each Member State's 2022 supervisory authority budget[63] by its 2024 population, providing a theoretically appropriate per-capita measure of regulatory investment.[64]

It is important to remark that Figure 2 presents fines per capita as a descriptive, secondary metric illustrating the uneven geographic distribution of GDPR penalties. While methodologically imperfect – since fines reflect numerous factors besides DPA strictness and population is not a theoretically meaningful denominator – this indicator reveals how sanction exposure concentrates unevenly across Member States. More robust factors behind enforcement intensity (such as DPA resources, caseload, decision-making patterns) are examined in the case studies below.

The graph highlights significant disparities in how Member States enforce the GDPR, both in the sum of monetary penalties per capita (blue bars) as well as in the total number of fines issued (red line). Countries such as France, Ireland, Germany, the Netherlands and Sweden have issued notably higher fines per citizen, indicating stricter enforcement or the imposition of substantial penalties on major violators. In contrast, countries such as Estonia, Latvia and Slovakia have issued significantly lower fines per capita, reflecting a more lenient or inconsistent application of GDPR sanctions.

Furthermore, there is a clear discrepancy between the number of fines issued and the total financial penalties per capita, with no direct correlation observed. Spain leads in the total number of fines issued, yet its per-capita fine amount is lower than high-enforcement states such as France and Ireland, suggesting that it imposes more frequent but lower-value fines. Meanwhile, Ireland and France impose fewer but significantly higher-value fines per capita, likely due to targeting large multinational corporations headquartered in their jurisdictions.

The yellow bars on DPA budget per capita reveal stark resource disparities. Luxembourg allocates €12.33 per capita, while most Member States invest less than €1. Spain's modest budget per capita (€0.35) shows how high-volume enforcement can be achieved with limited resources, whereas Latvia's relatively low allocation (€0.73) aligns with minimal output. These disparities demonstrate that enforcement patterns reflect institutional capacity alongside national legal frameworks and political priorities.

In summary, these findings indicate divergent enforcement strategies among Member States, where some focus on issuing numerous fines, while others prioritise imposing fewer but more substantial penalties. Such fragmentation underscores the challenge of GDPR enforcement, particularly in Member States hosting large multinational corporations, which tend to attract higher fines but may also benefit from regulatory leniency due to jurisdictional complexities.[65] This lack of

[62] CMS Law-Now, GDPR Enforcement Tracker.

[63] European Data Protection Board (EDPB), *Overview on resources made available by Member States to their data protection authorities*, 2022, https://www.edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf.

[64] Per-capita calculations use 2022 Supervisory Authority budget data (from the EDPB Report) and 2024 population figures (from Eurostat). Year-to-year population fluctuation is minimal (less than 2% for most Member States), so this temporal mismatch does not meaningfully affect the comparative analysis.

[65] Irish Council for Civil Liberties (ICCL), "5 years under the GDPR: Europe's enforcement paralysis", May 2023, https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf.

a unified approach to GDPR enforcement may lead to a regulatory patchwork, where companies use differences in enforcement strategies to their advantage. Such a fragmented application of digital law is inconsistent with the principle of the common data market that the legal framework seeks to establish.

6. Case studies

In analysing the implementation of the GDPR across Member States in case studies, this paper draws on Hill and Hupe's (2002) analytical framework of three levels of governance, which offers a structured view of the subject. The authors' model distinguishes between the constitutional level (design of political and administrative institutions), the directive level (policy formulation and maintenance of implementation trajectories), and the operational level (day-to-day management of inter-organisational relations and street-level practices).[66] This perspective is especially valuable for the following case studies, since it enables an analysis of each country's GDPR experience through the lens of its institutional relations; including how national implementation systems are designed, how national enforcement strategies are formulated, and how these supervisory authorities manage compliance in practice.

To justify this comparative design, the selection of Ireland, Spain, Italy and Latvia follows a variation-oriented sampling strategy grounded in GDPR enforcement relevance. These four Member States demonstrate diversity in size (large, medium, and small populations), institutional capacity (from highly resourced DPAs such as Spain's AEPD to one of the EU's smallest, Latvia's DVI), and prior regulatory traditions. These cases prove that enforcement outcomes may diverge because capacity, resources, and domestic fit matter.[67] Moreover, their markedly different fine volumes and per-capita sanction levels, as seen in Figure 2, reflect contrasting enforcement capacities, institutional priorities and pre-GDPR legal traditions that are worth analysing.

By examining Ireland, Spain, Italy, and Latvia through this lens, the analysis can connect the macro-level of legal design with the meso-level of institutional coordination and the micro-level of enforcement; thereby offering a systematic comparison of why enforcement patterns diverge across Member States. At the same time, this analytical framework is complemented by Hill and Hupe's top-down and bottom-up distinction. While GDPR represents a top-down regulatory mandate, its enforcement ultimately depends on bottom-up discretion and adaptation within national contexts.

6.1. Ireland

Ireland implemented the GDPR through the Data Protection Act 2018, repealing the country's older 1988–2003 data protection laws and transposing the EU Law Enforcement Directive in Parts 5–6. The 2018 Act also established a new institutional structure as the Data Protection Commissioner's office was expanded into a multi-member Data Protection Commission (DPC).[68]

Ireland in particular hosts the European or international bases of several Big Tech firms, making it a natural focal point for sanction-prone processing activities.

[66] Hill and Hupe, *Implementing public policy.*
[67] Lynskey, "Complete and effective data protection"; ICCL, "5 years under the GDPR."
[68] Department of Justice, Government of Ireland, Data Protection Act 2018, 25 May 2018.

The country's pre-GDPR regime was relatively modest, meaning the DPC had to scale up quickly to meet the GDPR's demands. This misalignment contributed to initial slow enforcement. For example, Ireland's regulatory culture of business-friendliness clashed with GDPR's strict enforcement ethos, requiring an adjustment period.[69] In implementation theory terms, Ireland experienced a *misfit* that caused delay until structures and resources caught up.[70]

As Ireland's supervisory authority, the DPC led many cross-border cases under GDPR's one-stop-shop mechanism. Ireland's cross-border GDPR caseload remains highly concentrated as, by 2022, nearly 87% of all incoming cross-border complaints related to only eight Big Tech firms. These include Meta (including WhatsApp), Google, Airbnb, Yahoo!, Twitter, Microsoft (including LinkedIn), Apple, and Tinder.[71]

While early enforcement drew criticism for slow throughput, attributed to heavy caseload and constrained resources that produced backlogs;[72] subsequent budget increases placed the DPC among the best-resourced EU DPAs. Concretely, Ireland's political commitment to strengthening GDPR enforcement is evident in the DPC's rapidly expanding budget, which increased from €15.2 million in 2019 to €26.36 million in 2023.[73]

Ireland's enforcement can therefore be described as structurally centralised and embedded in multi-level governance through the one-stop-shop. The DPC's draft decisions in major cross-border cases have repeatedly been escalated under Article 65 GDPR, with the EDPB directing tougher outcomes for a large share of Irish drafts, reflecting a supranational corrective to a nationally cautious stance. This also explains the combination of few but very large fines and lengthy timelines due to coordination with multiple concerned national DPAs. Many complaints continue to be resolved through reprimands or compliance orders, consistent with broader EU patterns.[74]

From an implementation-theory perspective, Ireland's GDPR trajectory illustrates the tension between top-down conformance and bottom-up problem-solving. The country faced an initial institutional misfit with its relatively modest pre-GDPR authority suddenly becoming the lead enforcer for Big Tech, exposing capacity deficits and political-economic sensitivities. In other words, from a top-down lens, Ireland formally complied via the Data Protection Act 2018, but in practice enforcement lagged behind EU expectations. However, the multi-level governance architecture of GDPR corrected this imbalance. The EDPB repeatedly overruled or toughened Irish draft decisions, showing how supranational oversight can compensate for domestic caution.[75] Ireland therefore embodies what Zürn and

[69] ICCL, "5 years under the GDPR."

[70] Tanja A. Börzel and Thomas Risse, "Conceptualizing the domestic impact of Europe", *The Politics of Europeanization* (2003): 57–80, https://doi.org/10.1093/0199252092.003.0003.

[71] ICCL, "5 years under the GDPR."

[72] Center for Strategic and International Studies (CSIS), *GDPR enforcement and the one-stop-shop* (Washington, DC: CSIS, 2021), https://www.csis.org.

[73] Data Protection Commission (DPC), *Annual report 2019* (Dublin: Data Protection Commission, 2020). Available at: https://dataprotection.ie/sites/default/files/uploads/2020-04/DPC%20Annual%20Report%202019.pdf; Data Protection Commission (DPC), *Annual report 2023* (Dublin: Data Protection Commission, 2024). Available at: https://www.dataprotection.ie/sites/default/files/uploads/2024-08/DPC-EN-AR-2023-Final-AC.pdf.

[74] Data Protection Commission (DPC), *Annual report 2019*; Data Protection Commission (DPC), *Annual report 2023* (Dublin: Data Protection Commission, 2024).

[75] Eva Thomann and Fritz Sager, "Moving beyond legal compliance: innovative approaches to eu

Joerges (2005) describe as the EU's legalised compliance regime; strong supranational corrective mechanisms sustaining compliance when domestic discretion risks under-enforcement.[76]

6.2. Spain

Spain swiftly adapted its legal framework to the GDPR with a landmark law known as the Organic Law 3/2018 of December 5, 2018 on Personal Data Protection and Guarantee of Digital Rights (LOPDGDD). This law not only aligns Spanish legislation with the GDPR but also expands on it by codifying new digital rights. Spain's Constitution (Article 18.4) had long established data protection as a fundamental right, and the LOPDGDD explicitly ties the exercise of that right to the GDPR as well as to the new national provisions. The law repealed the older 1999 Data Protection Act, modernising Spain's regime in one comprehensive statute.[77]

The AEPD serves as the national supervisory authority under the LOPDGDD while the Royal Decree 389/2021 (its Statute) clarifies the functions and use of GDPR powers. The LOPDGDD also tailors procedures domestically and enables DPO mediation prior to formal complaints. Uniquely, Spain also has regional data protection authorities in Catalonia, the Basque Country, and Andalucía that oversee public-sector data processing in those regions. The AEPD, however, handles the bulk of GDPR enforcement nationwide and coordinates with these autonomic authorities.[78]

Sustained political will translates into resources and procedural updates with a budget of around €17 million in 2022 as well as 2023 reforms to extend procedural timelines and create expedited reprimands to handle high volumes.[79] Civil society engagement is strong as consumer and digital-rights groups drive complaint inflows, and public debate around telemarketing, cookies, and CCTV feeds enforcement agendas. AEPD's *Memoria 2023* reports approximately 21,590 complaints (a 43% year-on-year increase), with concentrations in telecoms and internet services, and a sanctioning profile characterised by high volume and medium value relative to Big-Tech jurisdictions. Spain is thus a textbook multilevel governance case. Autonomous-community competences and dense domestic actor constellations (public & private) produce high complaint inflows and diversified enforcement.[80] Spanish doctrinal commentary similarly portrays Spain as a mature, enforcement-oriented regime. Data protection and privacy are entrenched constitutional fundamental rights and the AEPD has long combined significant sanctions with dense sector-specific guidance and guarantees for digital rights.[81]

---

multi-level implementation", *Journal of European Public Policy* 24, no. 9 (2017): 1253-1268, https://doi.org/10.1080/13501763.2017.1314541.

[76] Michael Zürn, and Christian Joerges, *Law and governance in postnational Europe: compliance beyond the nation-state* (Cambridge: Cambridge University Press, 2005).

[77] Recio, "Spain's new data protection law."

[78] Boletín Oficial del Estado. "Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos." *Boletín Oficial del Estado* 131 (June 1, 2021): 69271-69294, https://www.boe.es/eli/es/rd/2021/06/01/389/con.

[79] Agencia Española de Protección de Datos (AEPD), *Memoria 2023* (Madrid: AEPD, 2024), https://www.aepd.es/memorias/memoria-aepd-2023.pdf.

[80] AEPD, *Memoria 2023*.

[81] Leticia López-Lapuente and Reyes Bermejo Bosch, "Spain," in *The privacy, data protection and cybersecurity law review*, 7th ed., ed. Alan Charles Raul (London: Law Business Research Ltd., 2020), 372-386.

Moreover, Spain's experience exemplifies how formal alignment with EU law can coexist with practical pluralism in a decentralised unitary state. Multi-level competences generate diversified enforcement, consistent with the idea of Differentiated Policy Implementation, meaning patterned variation in how EU rules are applied across sectors and territories despite a shared legal framework.[82]

As for early enforcement of the GDPR, the AEPD simply gained even stronger tools, making the transition relatively seamless. For example, Spain was accustomed to issuing fines (which were frequent and sometimes hefty under its old law), therefore, the continuation under GDPR was a natural progression. This contrasts with countries that had to dramatically change their approach (high misfits). Spain reflects a case of high institutional fit, where EU-level requirements meshed with existing constitutional guarantees of data protection and a strong regulatory tradition. Moreover, the Spanish Organic Law 3/2018 going beyond mere transposition by ensuring new digital rights signals an embrace of domestication – or embedding supranational law into domestic settings – rather than minimal compliance.[83] Spain's AEPD, supported by regional authorities and active civil society, epitomises bottom-up problem-solving, where implementation is largely driven by public complaints and societal expectations.[84] Yet this responsiveness operates within a clear top-down mandate, producing both conformance and high-volume enforcement outcomes.

6.3. Italy

Italy approached GDPR transposition by amending its existing data protection code to align with the Regulation. The cornerstone of EU law implementation is the Italian Personal Data Protection Code (Legislative Decree 196/2003), which was substantially revised by Legislative Decree 101/2018, thereby adapting Italian data protection laws to the GDPR. Many national specifics (such as rules on employment data processing, journalism or scientific research) were updated but preserved, under the GDPR's allowances for Member State discretion.[85]

Italy's strong data protection tradition is deeply rooted in constitutional principles linking data protection to human dignity. The earlier Italian Data Protection of 2003 version explicitly declared in Article 1 that the goal of data protection law was the protection of dignity.[86] This constitutional grounding to link data protection and human dignity distinguishes Italy from other EU Member States and helps explain why the country developed such robust pre-GDPR protections.

Institutionally, the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) continued as the GDPR supervisory authority. The 2018 legal updates reinforced the *Garante's* powers in line with GDPR Article 58; including broad

[82] Asya Zhelyazkova, Eva Thomann, Eva Ruffing and Sebastiaan Princen, "Differentiated policy implementation in the European Union", *West European Politics* 47, no. 3 (2023): 439-465, https://doi.org/10.1080/01402382.2023.2257963.

[83] Zürn and Joerges, *Law and governance in postnational Europe.*

[84] Hill and Hupe, *Implementing public policy.*

[85] Jones Day, "Italian data protection decree harmonizes national law with the GDPR", 4 October 2018, https://www.jonesday.com/en/insights/2018/10/italian-data-protection-decree-harmonizes-national, Rocco Panetta, "Analysis: Italy's GDPR implementation law", International Association of Privacy Professionals (IAPP), 19 September 2018, https://iapp.org/news/a/analysis-italys-gdpr-implementation-law.

[86] Bart Custers and Gianclaudio Malgieri, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", *Computer Law & Security Review* 45 (2022): 1-13, https://doi.org/10.1016/j.clsr.2022.105683.

investigation authority, the ability to impose administrative fines up to GDPR's caps, and sanctioning powers for non-compliance.[87]

The Italian doctrinal scholarship therefore highlights a formalistic and procedurally rigorous data-protection culture.[88] In Differentiated Policy Implementation terms, Italy pairs a legalistic policy style with salient platform issues (such as high-profile political data use or digital platform cases) to produce assertive practical implementation; while EU-level mechanisms steer convergence in cross-border files.[89] Italy's GDPR story can be viewed through the lens of institutional fit and adaptation. The country had one of the strongest pre-GDPR data protection regimes. Accordingly, goodness-of-fit theory would predict the country's relatively smooth implementation, a case similar to Spain's.[90] Italy essentially translated the EU's requirements into its own legal language and already had the bureaucratic mechanisms to enforce them.

Italy therefore demonstrates continuity with enhancement. A well-developed pre-GDPR legal framework eased the incorporation of GDPR standards. From a top-down perspective, Italy experienced little friction, as the *Garante* was already empowered and culturally inclined towards legalistic enforcement. However, Italy also illustrates the performance-oriented, bottom-up dimension, where enforcement priorities reflect societal concerns. This is a blend of the processes of Europeanisation (the top-down pressure of EU rules) and domestication (how these rules are reinterpreted and adapted to national contexts).[91] Italy thus validates a hybrid implementation model, where both top-down conformance and bottom-up responsiveness reinforce each other.

6.4. Latvia

Latvia implemented the GDPR through a dedicated national law, the Personal Data Processing Law of June 2018, which took effect in July 2018. This law replaced the previous Personal Data Protection Law and provided the domestic legal scaffolding for GDPR application in Latvia. Key adaptations include specifying Latvia's Data State Inspectorate (Datu valsts inspekcija, DVI) as the supervisory authority and detailing its powers and procedures.[92]

A distinctive feature of Latvia's approach was an initial educational enforcement policy. In the first year after May 2018, the DVI emphasised guidance and warnings, especially for SMEs, instead of applying maximum fines. This strategy, codified in the country's law, was designed to ease businesses into compliance in a context of low awareness and limited administrative capacity. Latvia has a smaller, less platform-dense economy. Therefore, sanction exposure concentrates in conventional sectors (public bodies, SMEs, local online services).[93] Enforcement outcomes have been

[87] Garante per la Protezione dei Dati Personali, "I Poteri - Article 58 GDPR Powers", https://www.garanteprivacy.it/home_en.

[88] Giovanni Comandé and Giulia Schneider, "Differential data protection regimes in data-driven research: why the GDPR is more research-friendly than you think," *German Law Journal* 23, no. 4 (2022): 559–596, https://doi.org/10.1017/glj.2022.30.

[89] Zhelyazkova *et al.*, "Differentiated policy implementation in the European Union."

[90] Thomann and Sager, "Moving beyond legal compliance."

[91] Thomann and Sager, "Moving beyond legal compliance."

[92] DLA Piper, "Data protection laws in Latvia", *DLA Piper's Data Protection Laws of the World*, 4 February 2025, https://www.dlapiperdataprotection.com/?c=LV&t=law.

[93] OECD, *Going digital in Latvia: indicators of digital transformation and institutional readiness* (Paris:

modest, illustrating the authority's preference for corrective orders and warnings over sanctions, reflecting a more cautious enforcement trajectory.

The DVI's 2022 annual reports confirms that enforcement has relied primarily on corrective practices and guidance; with far more warnings, orders, and consultations than administrative fines. In the reporting period, 234 decisions were taken on corrective measures while only 16 administrative offence decisions were issued, demonstrating a strong preference for corrective orders over sanctions.[94]

Latvia's limited administrative capacity is central to this pattern. The DVI is one of the EU's smallest DPAs, with a 2022 budget of about €1.36 million. Such constraints prevent large-scale or complex investigations and force prioritisation of cases with immediate impact. Consequently, the DVI remains among the least-resourced EU supervisory authorities, curbing its enforcement output.[95] Coordination challenges seem to aggravate these limits as Latvia must devote resources to cross-border cooperation under the one-stop-shop system, responding to EDPB queries, and participating in joint operations.

From an implementation theory perspective, Latvia exemplifies a partial misfit between GDPR's ambitious enforcement design and its national capacity. While transposition was straightforward, enforcement has relied on bottom-up adjustment with education-first strategies and incremental sanctioning to match local contexts. This gradual build-up reflects bottom-up implementation models where national actors adapt EU rules pragmatically rather than applying them uniformly from the outset.[96] In multi-level governance terms, Latvia relies heavily on cooperation with the EDPB and larger DPAs, embodying Zürn and Joerges' (2005) insight that supranational legalisation provides smaller states with leverage but also imposes coordination burdens.[97] Latvia's case highlights the EU's differentiated implementation reality. Uniform rules generate diverse domestic practices shaped by capacity, discretion, and reliance on EU-level support.

In summary, across these case studies, GDPR implementation and enforcement diverge significantly; reflecting national legal frameworks, institutional strength, political context, and differing resources. Comparative analysis underscores the importance of institutional capacity and goodness-of-fit. Spain and Italy, with strong DPAs and privacy traditions, exhibited high institutional fit, allowing rapid and extensive enforcement. Ireland and Latvia, on the other hand, revealed greater misfits due to the unprecedented scope of supervising multinational technology platforms, scarce resources, and limited prior experience. EU rules alone did not seem to yield uniformity since national enforcement patterns are largely shaped by bottom-up pressures such as complaint flows, political will and tradition, as well as stakeholder mobilisation. Additionally, the quality of multi-level governance proved decisive. EDPB dispute resolution mechanisms tightened Ireland's decisions and smaller authorities like Latvia leveraged EU collective action to extend their reach. While the GDPR provides a uniform legal standard, its enforcement remains multi-faceted and uneven across Member States.

OECD Publishing, 2021), https://doi.org/10.1787/8eec1828-en.

[94] Datu valsts inspekcija (Data State Inspectorate), *Activity report 2022* (Riga: Datu valsts inspekcija, 2023), https://www.dvi.gov.lv/lv/media/3899/download?attachment.

[95] EDPB, *Overview on resources made available by Member States to their data protection authorities*, 2022.

[96] Zhelyazkova et al., "Differentiated policy implementation in the European Union."

[97] Zürn and Joerges, *Law and governance in postnational Europe.*

7. Concluding remarks

In conclusion, this article offers an interpretation of the main explanations behind the vulnerabilities of the GDPR in protecting individuals' personal data. Drawing on insights from the nature of personal data and how it interacts with other data points, it is proposed that, in its current form, the GDPR is prone to disregarding the risks of the de-anonymisation of data. With restrictive definitions of personal data, the law can ignore how combinations of anonymised data can ultimately yield personal data nonetheless.

On a theoretical level, EU data protection law should consolidate a risk-based and technologically grounded definition of anonymisation. One that is grounded in empirically demonstrable re-identification probabilities. Law must also clarify controller responsibilities when anonymised data is later shown to be re-identifiable alongside harmonised safeguards for sharing and re-using such datasets.

It is argued that, given the holistic legal framework concerning the data market, both the compliance by data handlers and individuals' ability to refer to their rights are hindered. This article has identified and provided examples of several acts that affect the rights of data subjects across the EU. Moreover, the different strategies of enforcement used by national authorities further distinguish the protection of data in Member States, thereby creating asymmetries in the protection of data subjects of different nationalities in a common data market.

With the RQs in mind, the GDPR's enforcement has unfolded unevenly, reflecting variations in institutional fit, administrative capacity, and regulatory traditions. With the help of theories of top-down and bottom-up implementation as well as goodness-of-fit; the comparative case studies of Ireland, Spain, Italy, and Latvia show how the implementation of the GDPR becomes differentiated across Member States and why such differences arise. In Ireland, institutional misfit and economic dependence on Big Tech slowed enforcement; strong institutional fit and high-volume enforcement characterised Spain; a robust pre-existing framework and immediate use of GDPR powers marked Italy; while limited administrative capacity and gradual enforcement defined Latvia. These findings demonstrate that the GDPR's formal uniformity masks diverse practical outcomes – which emerge from the interaction between EU rules and domestic institutions, political priorities, actors, and societal engagement.

In addition, the enforcement of GDPR fines varies significantly across Member States, with some imposing fewer but higher-value fines, often targeting major corporations, while others issue numerous lower-value penalties. These divergent strategies create inconsistencies in data protection enforcement; potentially undermining regulatory harmonisation, creating regulatory gaps that weaken deterrence, and incentivising businesses to seek jurisdictions with less stringent penalties.

From a more prescriptive standpoint, several reforms follow from this comparative analysis. For instance, the one-stop-shop mechanism would benefit from the introduction of binding cooperation deadlines and clear allocation of jurisdiction in cases that sit at the intersection of GDPR and digital privacy. Such clarity would help prevent situations in which data subjects fall between authorities. A reformed one-stop-shop would also provide predictable timelines for cross-border cases and limit regulatory bottlenecks in Big-Tech jurisdictions.

Procedural predictability should also extend to admissibility rules, the use of reprimands versus fines, and the rights of complainants during investigations. Novel regulatory mechanisms must ensure this practical harmonisation across Member States. As for minimum capacity standards for DPAs, mandatory baseline requirements could guarantee reasonable staffing, technical expertise, and annual budgets. These should be proportionate to population and cross-border caseload.

These recommendations align with – and could be reinforced by – the European Commission's Digital Omnibus and Digital Omnibus on AI Regulation from late 2025. These proposals aim to introduce binding cooperation deadlines, mandatory one-stop-shop procedures, accelerated dispute resolution, and clearer jurisdiction for e-privacy-adjacent cases.[98]

Importantly, these proposals corroborate the insight that substantive uniformity under the GDPR and digital rights law requires procedural standardisation as well as sufficient institutional resources. Yet these developments reinforce rather than resolve the analysed dynamics. Legal streamlining cannot, on its own, overcome the capacity disparities, political pressures, and definitional ambiguities that drive differentiated enforcement. Whether Member States apply some of these reforms strictly or leniently will still depend on the same structural factors identified in Sections 5–6; institutional capacity, political will, and domestic legal traditions.

Finally, despite the GDPR's comprehensive framework, establishing overarching principles in future regulation is crucial for setting ethical boundaries for emerging technologies and aligning data protection enforcement with societal values.

Article received on 27 October 2025 and accepted for publication on 18 November 2025.

[98] European Commission, Digital Omnibus, COM(2025) 837 final; European Commission, Digital Omnibus on AI, COM(2025) 836 final.