Marino R, Kashani SMM, Sadeghi F, 'Challenges and successes: General Data Protection Regulation (GDPR) implementation in Italy and Germany' (2025) Special Issue 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT25SIBRMSMMKFS

EJPLT
ISSN 2704-8012

Challenges and successes: General Data Protection Regulation (GDPR) implementation in Italy and Germany

Sfide e successi: attuazione del Regolamento Generale sulla Protezione dei Dati (GDPR) in Italia e Germania

ROBERTA MARINO
Full Professor of Private Law, University of Naples Federico II

SEYED MILAD MAHMOOD KASHANI
Ph.D. in Persons, Business and Markets Law, University of Naples Federico II

FATEMEH SADEGHI
Ph.D. (c) in Private Law, Arak Branch, Islamic Azad University

Abstract

The General Data Protection Regulation (GDPR) has significantly improved data security in the EU but has raised—since its adoption—numerous issues. Starting with the significant differences in the application of the GDPR between Italy and Germany, the contribution examines the main challenges that the two different domestic systems have had to face in relation to the GDPR, including the need to create legal uniformity and harmonize it with existing national legislation, as well as the issue of compliance costs. The issue of higher fines imposed under the GDPR is also addressed, finally providing information on the application models and their effects on businesses.

Il Regolamento generale sulla protezione dei dati (GDPR) ha migliorato notevolmente la sicurezza dei dati nell'UE, sollevando tuttavia – sin dalla sua approvazione- numerosi problemi. Muovendo dalle differenze significative nell'applicazione del GDPR tra Italia e Germania, il contributo esamina le principali sfide che i due diversi ordinamenti interni hanno dovuto affrontare in relazione al GDPR, tra cui la necessità di creare uniformità giuridica e di armonizzarla con la legislazione nazionale vigente, nonché la questione dei costi di conformità. Si affronta, inoltre, il tema delle sanzioni più elevate imposte ai sensi del GDPR fornendo, infine, informazioni sui modelli di applicazione e sui loro effetti sulle imprese.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: GDPR; Data Protection; Privacy; Germany; Italy.

Summary: 1. Introduction. – 2. Legal and cultural foundations of GDPR implementation. – 3. Challenges in GDPR Implementation in Italy and Germany. – 4. A Comparative Analysis of Italy and Germany. – 4.1 … and Germany. – 5. Comparison of Fines and Statistical Trends. – 6. Conclusion.

1. Introduction.[1]

Privacy and informational self-determination play a crucial role in protecting the consistency of an individual's identity and preventing sensitive information from proliferating into other contexts.[2] The protection of personal data is therefore essential not only for the free and self-determined development of the individual but also for safeguarding a free and democratic communication order. In this sense, the right to control one's own information has become a cornerstone of fundamental rights in the digital era.[3]

The data protection landscape has changed dramatically across Europe after the enforcement of the General Data Protection Regulation (GDPR) in 2018. GDPR is a privacy law at the heart of the EU that strives to establish a general standard of data protection, increase people's control over their information, and penalize organizations that misuse personal data. Yet, despite these ambitious objectives, the practical application of this sophisticated system has not been consistent within the member states.[4]

The analysis of its implementation demonstrates both common structural problems and significant national variations, raising the question of whether GDPR's promise of harmonization has been fully achieved.[5]

Against this background, two representative EU countries with distinct legal traditions – Italy and Germany – are chosen for closer examination. In the case of Italy, particularities of the legislative framework can be observed in the interplay between national laws and EU directives, whereas in Germany, a traditionally high level of concern for privacy has shaped the specific adaptation to GDPR. Both countries have faced challenges in implementing their legal frameworks, such as difficulties in ensuring uniform enforcement and tensions between national and supranational authorities. Nonetheless, they have also recorded notable improvements in the protection of personal data, offering valuable insights into the dynamics of legal adaptation.

The overall GDPR implementation experiences of Germany and Italy are therefore the central focus of this essay. By examining enforcement trends, regulatory activities, and corporate compliance, the paper aims to provide

[1] The Italian law sections are attributed to Roberta Marino, Professor of Private Law, University of Naples Federico II; the German law sections are attributed to Seyed Milad Mahmood Kashani, Ph.D. in Persons, Business and Markets Law, University of Naples Federico II and to Fatemeh Sadeghi, Ph.D. Candidate in Private Law, Arak Branch, Islamic Azad University.

[2] PK Donos, *Datenschutz–Prinzipien und Ziele. Unter besonderer Berücksichtigung der Entwicklung der Kommunikations-und Systemtheorie* (Baden-Baden 1998).

[3] N Luhmann, *Grundrechte als Institution.: Ein Beitrag zur politischen Soziologie* (2019).

[4] I Hanschke, *Information Security and Data Protection*, (1st edn, Wiesbaden 2019).

[5] J Pohle, *The still-relevant fundamental questions of data protection* (2014).

broad insights into how each of these countries engages with the complex requirements of modern data protection laws. In addition, statistics on the largest fines levied under GDPR are presented, not merely as descriptive data but as evidence for understanding enforcement patterns and their broader impact on business practices. In doing so, the paper contributes to the scholarly debate on whether GDPR has truly advanced the principle of informational self-determination in practice, or whether significant gaps remain between its normative ambitions and its actual enforcement.

2. Legal and cultural foundations of GDPR implementation.

The right to privacy refers to the principle that personal information must remain protected and that individuals are entitled to be left undisturbed in their private sphere. In today's digital society, however, an ever-increasing amount of personal information becomes accessible to third parties due to rapid technological advancements[6]. From e-commerce and email to mobile devices and social networks, new technologies constantly challenge both the legal system and societal expectations of privacy. At the same time, privacy is not merely a technical issue but a fundamental human right—one that underpins freedom of association, thought, and expression, as well as the right to live free from discrimination[7]. Yet, defining and safeguarding this right in practice remains highly complex.

The so-called information explosion of the twenty-first century is inseparable from the rise of cyberspace and, in particular, the global spread of the Internet[8]. In this new environment, geographical borders lose much of their meaning, and traditional conceptions of national sovereignty are significantly blurred. While the international community has generally resisted the idea of extending one nation's sovereignty over cyberspace, it has recognized the need for transnational frameworks to ensure security and stability online. This consensus has been reflected in a series of international conventions adopted under the auspices of the United Nations and other global bodies.[9]

A core objective of modern data protection laws, such as the GDPR, is to prevent data breaches and unauthorized access to personal information.[10] By mandating strict security requirements and establishing high standards of accountability, these regulations serve as a barrier against cyber threats and vulnerabilities. In the long run, they not only protect the integrity and confidentiality of personal data but also contribute to strengthening national

[6] E Horvitz, D Mulligan, 'Data, privacy, and the greater good' (2015) 349 Science 6245, 253-255.
[7] K El Emam, L Arbuckle, *Anonymizing Health Data: Case Studies and Methods to Get You Started* (O'Reilly Media 2013).
[8] V Zambrano, *I diritti della personalità. Manuale di diritto privato* (Giappichelli 2006) 309-347.
[9] PG Alpa, 'L'identità digitale e la tutela della persona. Spunti di riflessione' (2017) 33 Contratto e impresa, 723.
[10] D Messinetti, 'Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali' (1998) Rivista critica di diritto privato, 339–347; A Orestano, *La circolazione dei dati personali*, in R Pardolesi (ed), *Diritto alla riservatezza e circolazione dei dati personali*, (Giuffrè 2003), vol 2, 161; G Resta and V Zeno-Zencovich, Volontà e consenso nella fruizione dei servizi in rete, in Rivista trimestrale di diritto e procedura civile (2018) 432; L Mormile, Lo statuto giuridico dei dati personali, in R Panetta (ed) *Libera circolazione e protezione dei dati personali* (Giuffrè 2006) vol 1, 563.

cybersecurity infrastructures and ensuring reliable digital services for all stakeholders.[11]

Yet the debate on privacy cannot be limited to security concerns alone. The commercial dimension of personal data has emerged as an equally pressing issue. While many legal and philosophical traditions view personal data as an inalienable aspect of human identity—nontransferable, imprescriptible, and part of personality rights—market practices increasingly treat data as an economic asset.[12] In this perspective, user data are commodified, assigned a monetary value, and exchanged as part of bilateral negotiations in the digital economy. This tension between the inalienable character of personal data and the capitalization of data in commercial practice lies at the heart of contemporary debates on informational self-determination.[13]

As the collection of data expands for multiple purposes, its distribution becomes crucial for enhancing both its social and economic value. Applications ranging from smart cities to personalized commerce rely heavily on unprecedented levels of data sharing between individuals and organizations. [14] In contemporary society, therefore, data sharing is indispensable. At the same time, privacy concerns, security risks, and regulatory constraints necessitate a careful delineation of the parameters that govern such sharing.[15] The age of big data is marked not only by the exponential

---

[11] M Cocuccio, 'Il diritto all'identità personale e l'identità digitale', (2016) 3 Diritto di Famiglia e delle Persone, 949; G Resta, 'Identità personale e identità digitale', (2007) Diritto dell'informazione e dell'informatica 511–531; C Perlingieri, *Profili civilistici dei social networks* (ESI 2014) 88; G Resta and V Zeno-Zencovich, *Volontà e consenso*, ibid, 416.

[12] G D'Ippolito, 'Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale' (2020) 3 Il diritto dell'informazione e dell'informatica, 634.

[13] V Roppo, *Il contratto*, (2nd edn, Giuffrè 2011), 4–10, who seems to consider it possible to distinguish what is naturally patrimonial from what is not – according to an objective criterion – while at the same time admitting the possibility for the parties, in cases where it is lawful, to assign an economic value to agreements concerning matters that are not patrimonial in themselves. On this topic, see F Agnino, 'Fino a che punto è possibile disporre contrattualmente dei propri diritti? (Vedi contratto FB)', (2012) 2 Giurisprudenza di merito, 2559; V Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, I dati personali nel diritto europeo*, (Giappichelli 2019) 23

[14] K Liu et al., 'Enforceable Data Sharing Agreements Using Smart Contracts' (2018) *arXiv preprint* arXiv:1804.10645. Currently, however, we are witnessing a patrimonialisation of civil law, particularly with regard to fundamental rights which traditionally were attributed the characteristic of inalienability and non-patrimoniality and were consequently considered unable to interact with private autonomy, but are now subject to a process of patrimonialisation. In a diametrically opposite sense, distinguished scholarship proposed the category of depatrimonialisation to designate the progressive and increasingly marked sensitivity of contemporary private law, in all its components (legislative, doctrinal, jurisprudential), to data that cannot be confined within economic schemes and logics, even in areas traditionally reserved for patrimonial relations. C Donisi, 'Verso la "depatrimonializzazione" del diritto privato' (1980) Rassegna di diritto civile 644 ss. From here begins the "re-reading" of civil law institutions in a constitutional key carried out by our distinguished civil law scholarship. Among all, see P Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti* (3rd edn, ESI) 178; Id., 'L'informazione come bene giuridico' in P Perlingieri (ed), *Il diritto dei contratti fra persona e mercato* (ESI 2003) 353 ff.; These reflections are taken up by G Recinto, 'Il rilievo degli interessi non patrimoniali nel "difficile" rapporto tra autonomia negoziale e diritti della personalità' (2025) 1 Biblioteca della fondazione italiana del notariato 131. A De Franceschi and M Lehmann, 'Data as Tradeable Commodity and New Measures for their Protection' (2015) 1 The Italian Law Journal 51 ff; V Cuffaro, 'A proposito del ruolo del consenso', in V Cuffaro, V Ricciuto, V Zeno-Zencovich (eds), *Trattamento dei dati e tutela della persona* (Giuffrè 1998) 168, 121; A Di Majo, 'Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela' in V Cuffaro, V Ricciuto and V Zeno-Zencovich (eds), *Trattamento dei dati e tutela della persona* (Giuffrè 1998) 228 ff.

[15] V Ricciuto, 'La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno' in *I dati personali nel diritto europeo* (Giappichelli 2019) 23; On the economic value of data and their commercialization, see G D'Ippolito, Monetizzazione, patrimonializzazione e trattamento dei dati

growth of information but also by the increasing indispensability of sharing that information across borders and sectors.[16]

Technological progress has dramatically expanded the ability of businesses to collect, store, and exchange digitized data on a global scale. However, the complexity of data processing has also widened the asymmetry between data controllers and individuals.[17] Metadata generated from users' behaviors or even physical conditions illustrates how seemingly innocuous information can become highly sensitive. Under the earlier Directive 95/46/EC, [18] sanction policies proved insufficient to deter misuse, and national data protection authorities often lacked the resources to enforce more than a small portion of data processing activities.[19] Furthermore, the territorial scope of the Directive restricted European citizens' rights within Union borders, leaving cross-border data flows largely unaddressed. Self-regulatory mechanisms also failed to provide meaningful protection without binding enforcement.[20]

The General Data Protection Regulation (GDPR) was designed to remedy these shortcomings by strengthening accountability among data controllers and processors. It introduced obligations for documentation of processing activities, expanded territorial scope, and encouraged the adoption of certification procedures as evidence of compliance.[21] Each member state is required to establish one or more independent supervisory authorities responsible for monitoring and enforcing compliance. These authorities must cooperate closely with one another and with the European Commission, in accordance with Chapter VII of the Regulation, to ensure harmonized application across the Union.[22]

A central element of GDPR is the clear definition of personal data. Legally, personal data encompasses any information that relates to an identified or identifiable natural person or legal entity.[23] Within this category, sensitive data refers to information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, or sexual orientation. These categories receive heightened protection because of their intimate connection to individual dignity and autonomy. By contrast,

---

personali, in Cremona, Laviola, Pagnanelli (eds) *Il valore economico dei dati personali tra diritto pubblico e diritto privato* (Giappichelli 2022), 51; De Franceschi, Il "pagamento" mediante dati personali, in Cuffaro, D'Orazio, Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli 2020), 249 - 252; S Thobani, 'Operazioni di tying e libertà del consenso' (2019) Giurisprudenza italiana, 533.

[16] N Shibata et al., 'A method for sharing traffic jam information using inter-vehicle communication' (2006) 3rd Annual International Conference on Mobile and Ubiquitous Systems – Workshops (IEEE 2006) 1.

[17] C Walter, 'Kryder's law' (2005) 293(2) Scientific American, 32.

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

[19] BM Leiner et al., 'A brief history of the Internet' (2009) 39(5) ACM SIGCOMM Computer Communication Review, 22.

[20] S Arbesman, *Overcomplicated: Technology at the Limits of Comprehension* (Penguin 2017).

[21] N Nielsen, 'Hundreds of US Companies Make False Data Protection Claims' (8 October 2013) EUObserver

[22] M Gorge, 'Data protection: why are organisations still missing the point?' (2008) 2008(6) Computer Fraud & Security, 5; C Lo Surdo, 'Commento ai provvedimenti adottati dall'autorità garante in merito al problema del consenso informato' (1998) Danno e responsabilità 638–648.

[23] C Tikkinen-Piri, A Rohunen and J Markkula, 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34(1) Computer Law & Security Review, 134.

ordinary personal data, while less sensitive, remains essential to the exercise of privacy rights and informational self-determination.[24]

Finally, it must be emphasized that privacy protection extends beyond preventing the disclosure of confidential material. It encompasses all forms of information that relate to individuals, whether seemingly trivial or overtly sensitive. For this reason, governments must adopt precautionary measures not only in the physical sphere but also in the digital realm, ensuring that breaches of privacy—whether intentional or inadvertent—do not undermine the integrity of personal information.[25]

The General Data Protection Regulation (GDPR) has become a global benchmark for data protection laws and regulations. As the centerpiece of the EU's reform of the legislative framework for safeguarding personal data, it sets standards that are now recognized internationally.[26] Even beyond the EU's borders, many businesses voluntarily align with GDPR principles—particularly when targeting European customers or pursuing commercial interests in the EU. In this way, GDPR functions as a form of "regulatory export," extending its influence far beyond Europe.[27]

Nevertheless, the reality of information leakage underscores the limits of even the most advanced frameworks. Data is inevitably lost, stolen, or misused, often with malicious intent. Under GDPR, organizations are not only required to collect personal data under lawful and clearly defined conditions but are also obligated to safeguard it against exploitation.[28] Failure to comply results in significant sanctions. These strict requirements reflect the growing global recognition of personal data protection as an urgent issue. In fact, many developing countries are now adopting mandatory biometric data systems, raising both opportunities for identity management and new concerns about privacy rights.

The collection of vast amounts of sensitive personal data by researchers, corporations, and governments has introduced unprecedented threats to individual privacy and data security. Traditional centralized data systems often lack adequate transparency, accountability, and user control, thereby enabling the repurposing of personal data for mass surveillance and even censorship. In response, data protection authorities within the EU have sought to clarify the legitimate boundaries of data use. The European Data Protection Board, for instance, has issued guidance on the protection of personal information, emphasizing the necessity of both transparency and accountability.[29]

---

[24] P Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Springer International Publishing 2017); F Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' (2017) Nuove leggi civili commentate, 401.

[25] L Raisi Dezaki and F Ghasemzadeh Liasi, 'Challenges of Iran's legal system in violation of personal data and privacy in cyberspace' (2019) 110 Judicial Law Journal, 123.

[26] C Kuner et al., *The EU General Data Protection Regulation: A Commentary* (Updated Selected Articles, 4 May 2021, 2020).

[27] P Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Springer International Publishing 2017).

[28] I Ekong, E Chukwu and M Chukwu, 'COVID-19 mobile positioning data contact tracing and patient privacy regulations: exploratory search of global response strategies and the use of digital tools in Nigeria' (2020) 8(4) JMIR mHealth and uHealth e19139.

[29] B de A Almeida et al., 'Personal data usage and privacy considerations in the COVID-19 global pandemic' (2020) 25 Ciência & Saúde Coletiva, 2487.

At the heart of GDPR lies the requirement for a legal basis in any collection or use of personal data belonging to EU citizens and residents. Among the available legal grounds, consent occupies a fundamental role. However, GDPR strictly defines valid consent: it must be freely given, specific, informed, and unambiguous. This framework attempts to restore balance between data subjects and controllers by ensuring that individuals retain meaningful control over their personal information.[30]

Ultimately, GDPR empowers individuals to regulate how their data is accessed and processed. Smart devices, cloud-based services, and other digital platforms are obliged to obtain clear user permission before altering or processing personal data.[31] This represents not only a shift in regulatory emphasis but also a broader cultural change, in which the protection of informational self-determination is increasingly recognized as essential for democratic societies in the digital age.[32]

3. Challenges in GDPR Implementation in Italy and Germany.

The General Data Protection Regulation (GDPR) builds upon the fundamental goals and principles of the Data Protection Directive 95/46/EC (DSRL), first adopted in 1995. Many of its core provisions remain familiar: Article 5 reiterates the basic principles of lawful data processing, Article 6(1) preserves the general conditions for permissible processing, and Article 9 continues to regulate special categories of sensitive personal data.[33] Likewise, Articles 12 to 23 strengthen the rights of individuals in relation to their data, largely reformulating rather than revolutionizing earlier provisions. In this sense, GDPR represents an evolutionary step rather than a radical departure, clarifying, consolidating, and extending existing rules rather than conceptually reinventing them.[34]

Despite this continuity, the Regulation introduces ambitious new objectives. Its twofold mission is, first, to safeguard the fundamental rights and freedoms of individuals—especially the right to personal data protection—and second, to guarantee the free flow of personal data within the EU, eliminating national

[30] O Park et al. 'Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts (2020) (11) 1 Osong Public Health Res Perspect, 60 – 63. DOI: https://doi.org/10.24171/j.phrp.2020.11.1.09

[31] P Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Springer International Publishing 2017); V Zeno-Zencovich, Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante, (1997) Corriere giuridico, 919; IA Caggiano, 'Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale' (2018) 1 Osservatorio del diritto civile e commerciale, 73; A Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale*, (ESI 2019); C Basunti, 'La (presunta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali' (2020) Contratto e impresa, 860; A Purpura, 'Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data', (2022) 4 Jus civile, 901 ss.

[32] M Barati et al., 'GDPR compliance verification in internet of things' (2020) 8 IEEE Access, 119697.

[33] A Benecke and J Wagner, 'Opening Clauses in the General Data Protection Regulation and the German Federal Data Protection Act – Limits and Scope for National Data Protection Law' (2016) 131(10) Deutsches Verwaltungsblatt, 600.

[34] M Martini and J Kühling, 'The General Data Protection Regulation: Revolution or Evolution in European and National Data Protection Law?' (2016) 27(12) European Journal of Business Law (EuZW) 448.

restrictions that could fragment the internal market.[35] At the same time, the GDPR places restrictions on transfers of personal data to third countries, authorizing them only when the European Commission deems the recipient jurisdiction to offer an adequate level of protection.[36]

To achieve these aims, GDPR imposes a series of compliance mechanisms. These include mandatory data protection impact assessments, the appointment of data protection officers in certain organizations, and the obligation for most controllers to maintain registers of data processing. It also sets out strict rules on breach notifications and grants supervisory authorities significant enforcement powers. [37] Authorities may impose temporary or permanent bans on processing and, in the most serious cases, issue administrative fines of up to €20 million or 4% of a company's global annual turnover.

Yet these very provisions that appear clear at the EU level have proven challenging in practice within member states such as Italy and Germany. Differences in administrative capacity, enforcement traditions, and legal cultures mean that the "uniform" framework of GDPR often encounters diverging interpretations and practical difficulties. These divergences form the basis of the challenges explored in the following subsections.[38]

The General Data Protection Regulation assigns supervisory authorities a central role in ensuring compliance. Their responsibilities include preventive monitoring, raising public awareness, advising governments on legislative initiatives, and carrying out data protection impact assessments.[39] They must also inform individuals about risks, protective measures, and their rights under the Regulation. To achieve this, supervisory authorities are expected to develop effective communication strategies and maintain an active presence in public debates on privacy. These functions are not peripheral but integral to GDPR's implementation framework.[40]

In addition, supervisory authorities are empowered to intervene directly in cases of non-compliance. They may notify controllers or processors of suspected breaches, issue warnings when processing activities appear unlawful, and impose corrective measures where necessary. To facilitate compliance, organizations are required to designate Data Protection Officers (DPOs), who act as the primary point of contact with supervisory authorities.[41] DPOs advise organizations on their obligations, ensure internal alignment with GDPR principles, and seek clarification from regulators when uncertainties arise. A constructive partnership between supervisory authorities and DPOs is

[35] Goodell, Geoff, and Tomaso Aste, 'Can cryptocurrencies preserve privacy and comply with regulations?'. (2019) 2 Frontiers in Blockchain 4.
[36] J Kaufmann and W Rechtsanwälte, *Blockchain meets Data Privacy (Part 1)* (2018).
[37] A von dem Bussche and A Zeiter, 'Implementing the EU general data protection regulation: a business perspective' (2016) 2 European Data Protection Law Review 576.
[38] WG Voss, 'Internal compliance mechanisms for firms in the EU General Data Protection Regulation' (2016) 50 Revue Juridique Thémis 783.
[39] U Dammann, 'Erfolge und Defizite der EU-Datenschutzgrundverordnung: Erwarteter Fortschritt, Schwächen und überraschende Innovationen' (2016) Zeitschrift für Datenschutz (ZD) 307.
[40] JP Albrecht, 'Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung' (2016) 32(2) Computer und Recht 88.
[41] T Bittner, 'Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf' (2014).

therefore indispensable, based on mutual trust and continuous exchange of information.

Articles 37 to 39 of the GDPR specify when the appointment of a DPO is mandatory: for public authorities, for organizations engaged in systematic large-scale monitoring of individuals, or for those processing large volumes of sensitive or criminal data.[42] Once appointed, the DPO must oversee training, risk management, and compliance procedures, while also leading the Data Protection Impact Assessment (DPIA) process.[43] The DPO further serves as an intermediary for complaints and requests from data subjects, ensuring that individual rights are respected in practice.

While these provisions establish a comprehensive compliance architecture, their implementation has posed significant challenges in both Italy and Germany. In practice, supervisory authorities in these countries face constraints of resources and administrative capacity, while many organizations—particularly small and medium-sized enterprises—struggle to meet the expectations placed on DPOs.[44] Moreover, cultural differences in regulatory traditions shape how actively these duties are enforced: Germany, with its strong privacy culture, has developed a more robust DPO system, whereas Italy has encountered difficulties in creating effective awareness and communication strategies. These contrasts illustrate how uniform EU rules often yield diverse national experiences in practice.[45]

For the role of Data Protection Officer (DPO) to be effective, it must be exercised with a high degree of autonomy. Organizations are required to provide adequate resources, access to information, and training to ensure that the DPO can fulfill their responsibilities. A DPO may be appointed internally or contracted externally, but in either case, they must remain constantly updated on relevant laws, policies, and enforcement practices.[46] Their responsibilities extend beyond mere compliance: they are essential to building public trust and safeguarding the reputation of organizations, particularly those processing large volumes of sensitive data.[47]

While the GDPR established a uniform baseline for data protection across the EU, its implementation has revealed practical difficulties for companies, especially with regard to cross-border data flows. Firms often struggle to reconcile GDPR requirements with the specific provisions of national legislation, creating uncertainty about the applicable standards in different jurisdictions.[48] Recognizing these challenges, the European Commission has

[42] C Klug, 'Der Datenschutzbeauftragte in der EU – Maßgaben der Datenschutzgrundverordnung' (2016) Zeitschrift für Datenschutz (ZD) 315.
[43] P Laue, S Kremer and J Nink, *Das neue Datenschutzrecht in der betrieblichen Praxis* (Nomos 2016).
[44] K Marschall and P Müller, 'Der Datenschutzbeauftragte im Unternehmen zwischen BDSG und DSGVO – Bestellung, Rolle, Aufgaben und Anforderungen im Fokus europäischer Veränderungen' (2016) 6(9) Zeitschrift für Datenschutz (ZD) 415.
[45] A M Nguyen, 'Die zukünftige Datenschutzaufsicht in Europa' (2015) 5(6) Zeitschrift für Datenschutz (ZD) 265.
[46] C Kuner et al., The EU General Data Protection Regulation: A Commentary (Updated Selected Articles, 4 May 2021, 2020).
[47] P Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Springer International Publishing 2017).
[48] CA Giusti and FL Giambrone, 'The Data Protection Framework in Germany for the Operation of Evaluation Platforms on the Internet on the Basis of the GDPR (General Data Protection Regulation)' (2022) 28(2) The Cardozo Electronic Law Bulletin.

emphasized the need for a unified and binding framework to achieve two overarching objectives:[49]

1. Safeguarding the fundamental rights, privacy, and freedoms of individuals across the EU.
2. Promoting the unhindered flow of data within the Union, thereby reducing barriers to business operations.

However, in practice, both Italy and Germany have faced obstacles in realizing these goals. In Italy, limited institutional capacity and uneven enforcement practices have hindered the full integration of GDPR into domestic systems. In Germany, by contrast, a strong privacy culture has encouraged strict interpretation of GDPR provisions, but this has also created compliance burdens for businesses operating across multiple Länder (federal states). These differences demonstrate how the same European rules, when filtered through distinct legal and administrative contexts, give rise to divergent national challenges.

4. A Comparative analysis of Italy…

In Italy, the primary legislative framework governing privacy and data protection is the Codice in materia di protezione dei dati personali (Personal Data Protection Code). [50] This law, which predates the GDPR, introduced comprehensive requirements for both public and private sector organizations regarding the collection and processing of personal information. It clearly distinguished between two key actors: data controllers and data processors. Controllers were given full autonomy to determine the purposes and means of processing operations, as well as responsibility for ensuring adequate security measures. Processors, by contrast, were appointed by controllers and could only act under their instructions.[51]

The GDPR reinforced and harmonized these roles across the European Union, but their interpretation and enforcement in Italy remained closely tied to the existing national framework. [52] Under Articles 4 and 24–28 of the Regulation, the data controller—whether a natural person, legal entity, or public authority—decides why and how personal data should be processed, and

[49] LA Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002) 316.
[50] S Rodotà, Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy (2004) Eur. dir. priv. 4 ss.; CM Bianca and FD Busnelli (eds), *La protezione dei dati personali. Commentario al D Lgs 30 giugno 2003, n 196 («codice della privacy»)*, I (CEDAM 2007); Currently, the regulation on the protection of personal data in Italy is based on the combined provisions of d. lgs. 196/2003 and Regulation 2016/679. The Privacy Code, amended following EU Regulation 2016/679, required the introduction of internal implementing provisions, in particular d. lgs. 10 August 2018, no. 101, entitled "Provisions for the adaptation of national legislation to the provisions of 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)", which entered into force on 19 September 2018. This decree made the necessary amendments to coordinate with d. lgs. 196/2003, which, as mentioned, remains in force. G. Alpa, *La disciplina dei dati personali. Note esegetiche sulla legge 31 dicembre 1996, n. 675 e successive modifiche* (Seam 1998) 90;
[51] B Custers et al., 'A comparison of data protection legislation and policies across the EU' (2018) 34(2) Computer Law & Security Review 234.
[52] P Balboni, *Privacy and Data Protection Law in Italy* (Kluwer Law International BV 2024).

thus carries primary responsibility for compliance.[53] Controllers must ensure transparency, obtain valid consent where necessary, and uphold data subject rights, including access, rectification, and erasure. Even when controllers outsource technical operations to processors, they retain ultimate accountability for lawful processing.[54]

By contrast, the data processor may only act on instructions from the controller and is prohibited from using personal data for independent purposes.[55] Processors must adhere to contractual obligations, implement robust security measures, and report data breaches without undue delay. A typical example is the relationship between a bank and its cloud storage provider: the bank, which defines the objectives and legal grounds of data processing, acts as the controller, while the cloud provider functions as the processor under contract.[56]

In the Italian context, this distinction has been essential for clarifying compliance obligations, but it has also presented challenges. Many small and medium-sized enterprises (SMEs) have struggled to fully understand the extent of their responsibilities as controllers, often underestimating the need for documentation and proactive risk management.[57] The Italian Data Protection Authority (Garante per la protezione dei dati personali) has repeatedly emphasized that ultimate accountability lies with the controller, regardless of outsourcing, highlighting one of the recurring obstacles in Italy's adaptation to the GDPR.[58]

In Italian law, personal data is broadly defined as any information relating to an identified or identifiable natural person. Identification may occur directly—

---

[53] S Niger, 'Note sul diritto alla protezione dei dati personali' (2004) Ciberspazio e diritto 49 ff; S Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali* (CEDAM 2006) 63 ff.

[54] R Carleo, Il principio di accountability nel GDPR: dalla regola alla auto-regolazione (2021) Nuovo diritto civile, 356, observes that the GDPR is characterized by its approach based on the principle of accountability, that is, on the responsibility of the data controller, who is required to implement "appropriate" technical measures to ensure a level of security corresponding to the risk. The controller's responsibility is divided between the assessment and adoption of suitable security measures and the conduct of continuous monitoring, also through the elaboration of specific organizational models. In addition, the controller must be able to demonstrate everything, proving the adequacy of the regulatory choices made autonomously. Accountability, which may be translated as "responsibility and, at the same time, proof of responsibility," is a two-level mechanism: one of implementing measures, the other of preserving evidence. It should not be overlooked that, pursuant to Articles 83 and 84 GDPR, the failure by the controller to adopt appropriate technical and organizational (including security) measures results in heavy administrative fines, and the violation of these obligations determines aggravated liability for presumed fault of the controller (and processor) and, consequently, the obligation to compensate for damages under Article 82. See, G Finocchiaro, Intelligenza Artificiale e protezione dei dati personali (2019) Giurisprudenza Italiana 1675 ff. See also M Gambini, Responsabilità civile e controlli del trattamento algoritmico, in P Perlingieri, S Giova and I Prisco (eds), *Il trattamento algoritmico dei dati tra etica, diritto e economia* ESI 2020); P Perlingieri, S Giova and I Prisco (eds), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità* (ESI 2020) 330 ff.

[55] V Zeno-Zencovich, G Giannone Codiglione, 'Ten legal perspectives on the "big data revolution"' (2016) 23 Concorrenza e mercato 29 ff.

[56] P Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Springer International Publishing 2017).

[57] C Tikkinen-Piri, A Rohunen and J Markkula, 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34(1) Computer Law & Security Review 134; A Mantelero, *Il costo della privacy tra valore della persona e ragioni d'impresa* (Giuffrè 2007) 318 ff.

[58] A Frosini, 'Gli atti normativi del Garante per la protezione dei dati personali' (2014) Giurisprudenza Costituzionale; A Pirozzoli, 'Il potere di influenza delle Autorità amministrative indipendenti' (2017) 23 Federalismi.it; G Napolitano, 'A trent'anni dal "trapianto" delle autorità indipendenti in Italia: innesto riuscito o crisi di rigetto?' in *Liber Amicorum per Marco D'Alberti* (Giappichelli, Torino 2022) 188 ff.

for example, through a fiscal code—or indirectly, by reference to other data such as an IP address. However, once information is rendered truly anonymous and can no longer be linked to an individual by any means, it falls outside the scope of the Italian Data Protection Code.[59] This distinction, though clear in principle, has raised significant practical challenges, particularly as modern technologies make it increasingly difficult to guarantee full and irreversible anonymization.

The territorial scope of the Italian framework is also noteworthy. The Codice in materia di protezione dei dati personali applies not only to processing operations carried out within Italian territory, but also to controllers and processors located abroad if they use equipment or tools situated in Italy. In such cases, foreign controllers must appoint a local representative to ensure compliance with Italian law. While this provision aimed to strengthen protection, it has created compliance burdens for multinational companies operating in Italy, especially in sectors such as telecommunications and digital services.[60]

The Italian Code, first enacted in 2003 through Legislative Decree No. 196/2003, [61] represented a pioneering attempt to consolidate privacy protections at the national level. Following the entry into force of the GDPR in May 2018, the Code was significantly amended to align national rules with the new European standard. Despite this alignment, Italian authorities and businesses have faced interpretive difficulties in reconciling national provisions with the broader obligations of the GDPR.[62] For example, the question of how to balance Italy's expansive territorial scope with GDPR's extraterritorial provisions remains an ongoing source of uncertainty in both legal doctrine and enforcement practice.

As an EU regulation, the GDPR applies directly across all member states, including Italy. The Italian Personal Data Protection Code complements the GDPR by addressing areas not explicitly regulated at the European level and by ensuring consistency with Italy's legal and administrative traditions. Enforcement is overseen by the Italian Data Protection Authority (Garante per la protezione dei dati personali), which monitors compliance, investigates complaints, issues fines, and provides interpretative guidance. [63] Thanks to the Garante's active role, Italy has developed a reputation for robust enforcement and a rigorous approach to safeguarding personal data.

The Italian framework applies broadly to both governmental and private sectors, with its key principles emphasizing that all data processing must respect the rights, freedoms, and dignity of individuals. Special protection is

[59] N Maccabiani, 'Testing governance and its regulatory techniques against some of the GDPR provisions' (2021) 21 Federalismi.it, 147.
[60] F Rossi Dal Pozzo, 'Big Data and Public Law: New Challenges Beyond Data Protection' (2019) Eurojus (Special Issue) 1.
[61] Italian Government, Italian Personal Data Protection Code: Legislative Decree no. 196 of 30 June 2003 [2003] (accessed via Privacy.it).
[62] K Wiedemann, 'Maria Cristina Caldarola / Joachim Schrey: Big Data and Law: A Practitioner's Guide '(2021) 210–211.
[63] P Guarda, 'Data Protection, Information Privacy and Security Measures: an Essay on the European and the Italian Legal Frameworks' (2008) 9(1) Ciberspazio e Diritto: Internet e le Professioni Giuridiche 65.

afforded to confidentiality, personal identity, and access rights. [64] Nevertheless, the practical application of these principles has not been without controversy. For example, the Agenzia delle Entrate (Italian Revenue Agency) has been criticized over the past decade for extensive use of personal information in efforts to combat tax evasion. The Garante argued that such practices risk disproportionately infringing upon fundamental rights, highlighting the tension between privacy and state interests in financial control.[65]

In 2018, Italy also introduced a number of derogations under Article 23 of Legislative Decree No. 101/2018, the law aligning national rules with GDPR. Particularly significant is Article 2-undecies, letter D, which permits government authorities and financial intermediaries to limit certain data subject rights under Articles 15–22 of the GDPR in order to protect the integrity of financial and payment systems.[66] While these exceptions are justified as necessary safeguards, critics argue that they risk undermining the very essence of GDPR's data subject rights and disproportionately favor institutional actors over individuals. This tension illustrates one of the central challenges in Italy's implementation of GDPR: balancing the protection of personal freedoms with competing economic and administrative interests.[67]

4.1 … and Germany.

In Germany, the issue of data protection gained prominence with the rapid automation of information processing in the post-war decades. Since the 1950s, authorities in the social security and tax systems had begun using emerging computer technologies to collect and analyze personal information, with the aim of improving forecasting and planning.[68] While these innovations enhanced administrative efficiency, they also triggered widespread concerns about the expansion of state "information power" (Informationsmacht) and the erosion of individual privacy.[69] This climate of apprehension fueled early demands for stronger legal safeguards and explains why Germany became a pioneer in the field of data protection.

The rise of data protection as a political concern coincided with Germany's broader transition to a post-industrial economy in the 1960s. As governments increasingly relied on computerized data to manage social and economic change, the relationship between the state and the individual was

[64] L Jarvis, *The Age of Big Data Analytics: A Cross-National Comparison of the Implementation of Article 23 of the GDPR in the United Kingdom, France, Germany and Italy* (2019); F Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, (CEDAM 2018), 44; G Versaci, *La contrattualizzazione dei dati personali dei consumatori*, (ESI 2020).
[65] K. Mc Cullagh, O. Tambou, S. Bourton (eds.), *National Adaptations of the GDPR*, (Collection Open Access Book, Blogdroiteuropeen, Luxembourg 2019).
[66] DJ Felz, 'An English Language Primer on Germany's GDPR Implementation Statute: Part 2 of 5' (25 September 2017, accessed 5 May 2018).
[67] L Jarvis, *The Age of Big Data Analytics: A Cross-National Comparison of the Implementation of Article 23 of the GDPR in the United Kingdom, France, Germany and Italy* (2019).
[68] K von Lewinski, 'Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive' in J-H Schmidt and T Weichert (eds), *Datenschutz: Grundlagen, Entwicklungen und Kontroversen* (Bundeszentrale für politische Bildung 2012) 23.
[69] J Taeger and D Gabel, *DSGVO–BDSG* (Deutscher Fachverlag 2019).

fundamentally redefined.[70] In 1970, the State of Hesse adopted the world's first data protection law, marking a decisive moment in the legal recognition of privacy as a fundamental right in the information age.[71]

This momentum led to the passage of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG[72]), approved by the German Parliament in 1977 and effective as of January 1, 1978. The BDSG consolidated data protection at the national level, but it was not without limitations[73]. The original law defined data processing narrowly, focusing on the use of information rather than its collection, and it failed to establish the principle of purpose limitation, which later became central under the GDPR. These shortcomings prompted subsequent reforms in 1991 and again in 2000, as Germany sought to expand protections in light of new technological developments and the growing importance of cyberspace.[74]

Under German data protection law, the collection of personal data by public authorities is permitted only when the purpose of processing is made clear to the data subject. The principle of purpose limitation requires that the collection must align with the legitimate objectives of the collecting organization, and subsequent use or storage is lawful only if the initial collection was conducted transparently and on a proper legal basis. Any processing that occurs without the citizen's knowledge or for undisclosed purposes is considered unlawful[75]. In this framework, disclosure is classified as the "transfer of personal data" and is permissible solely when necessary and restricted to the pre-determined purposes for which the data was originally gathered.

A distinctive feature of Germany's data protection regime lies in its federal structure. Responsibility is shared between the federal government and the sixteen Länder (states), each of which maintains its own supervisory authority and legal framework.[76] These state-level authorities operate with considerable autonomy, creating a patchwork of enforcement practices. At the national level, the Federal Commissioner for Data Protection and Freedom of Information, headquartered in Bonn, represents Germany on the European Data Protection Board. While this decentralized model reflects Germany's federalism, it has also produced uneven interpretations and enforcement of

[70] B Van Alsenoy, *Regulating Data Protection: The Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing* (2016).
[71] Union européenne. Agence des droits fondamentaux, Conseil de l'Europe, and Cour européenne des droits de l'homme. Handbook on European data protection law. Publications office of the European Union, 2014.
[72] German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).
[73] Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045) [Federal Law Gazette] (accessed via Gesetze-im-Internet) (https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html)).
[74] S Fischer-Hübner (ed), *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms* (Springer Berlin Heidelberg 2001).
[75] V Akefi Ghaziani, M Akefi Ghaziani and M Akefi Ghaziani, 'Assessing Non-Material Damages Under the GDPR: A Review of the Recent Judicial Practice of Germany, UK, and the Netherlands' (2022) Revista Jurídica Portucalense 274.
[76] G Hornung and C Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25(1) Computer Law & Security Review 84.

GDPR provisions, leading to regulatory uncertainty for organizations operating nationwide.[77]

Germany's enforcement record underscores both the strength and fragmentation of its system. The first confirmed GDPR fine was issued by the supervisory authority of Baden-Württemberg against a social networking company for inadequate data security measures.[78] Subsequent fines by Berlin, Hamburg, Saxony-Anhalt, and other Länder authorities reveal an assertive enforcement stance, though with notable differences in scope and severity. The most prominent case to date remains the €14.5 million fine imposed in 2019 by the Berlin Data Protection Authority on the property rental company Deutsche Wohnen for unlawful data retention practices. Between May 2018 and February 2019 alone, Länder authorities imposed at least 41 fines, illustrating Germany's commitment to rigorous enforcement, but also highlighting the challenge of coordinating such actions across multiple jurisdictions.[79]

In Germany, oversight of data protection reflects the country's federal structure and its strong constitutional tradition. At the federal level, the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) is responsible for monitoring compliance by federal government bodies, with its powers defined in Sections 22–26 of the Federal Data Protection Act (BDSG)[80]. Alongside this federal authority, each of the sixteen Länder has its own Data Protection Commissioner, who supervises both public authorities within the state and private-sector organizations operating locally. This decentralized model reflects Germany's constitutional commitment to federalism, but it also introduces complexity and, at times, uneven application of GDPR provisions across regions.[81]

To ensure compliance within organizations themselves, both public and private entities are required to appoint Data Protection Officers (DPOs). These internal officers monitor adherence to data protection rules, advise management, and serve as points of contact for supervisory authorities. The DPO system is regarded as one of Germany's most distinctive contributions to the European data protection landscape, embedding accountability directly into organizational structures.[82]

The German Federal Constitutional Court has played a decisive role in shaping this framework. In its landmark Census Act ruling of 1983, the Court articulated the fundamental right to informational self-determination, holding that any interference must respect the principles of proportionality and

[77] W Hartzog and N Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 Boston College Law Review 1687.
[78] O Schmidt, 'Germany's first fine under the GDPR offers enforcement insights' (27 November 2018) International Association of Privacy Professionals.
[79] W Schulz, 'Regulating intermediaries to protect privacy online – the case of the German NetzDG' (Forthcoming 2018) Personality and Data Protection Rights on the Internet.
[80] G Hornung and C Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25(1) Computer Law & Security Review 84.
[81] R Gellert, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5 International Data Privacy Law 3.
[82] C DeSimone, 'Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive' (2010) 11(3) German Law Journal 291.

procedural safeguards. The Court emphasized the necessity of independent supervisory authorities capable of exercising effective control over data processing activities. [83] This jurisprudence established a constitutional foundation for Germany's insistence on strong, independent oversight mechanisms—both at the supervisory authority level and within organizations through DPOs.

Yet, this layered system also poses challenges. The multiplicity of supervisory bodies can create divergent enforcement approaches, generating uncertainty for companies operating nationwide. At the same time, the heavy reliance on internal DPOs places significant compliance burdens on smaller organizations, which may lack the resources to sustain full-time data protection expertise.[84] Thus, while Germany's model is often praised as the most rigorous in Europe, it also illustrates the trade-off between robust constitutional protection and practical feasibility of implementation.

Germany's approach to GDPR implementation reflects both its pioneering tradition in data protection and the structural challenges of its federal system. On the one hand, the German model is marked by rigorous safeguards: individuals can lodge complaints with independent supervisory authorities, and associations are empowered to represent data subjects free of charge under Article 80 GDPR. The Federal Data Protection Act (BDSG) and recent reforms have expanded the authority of supervisory bodies to investigate complaints, initiate legal proceedings, and even involve public prosecutors in cases of serious breaches.[85] These mechanisms underscore Germany's commitment to strengthening informational self-determination as a constitutional right.

On the other hand, enforcement in practice reveals significant institutional weaknesses. Supervisory authorities often lack the staff and resources to pursue complaints effectively, and criminal proceedings for data protection violations are rarely sustained by public prosecutors or courts.[86] The heavy reliance on associations to defend data subject rights risks overwhelming supervisory authorities with new claims, further stretching their limited capacity. Moreover, Germany's fragmented enforcement structure—split between federal and Länder authorities—creates inconsistencies that complicate compliance for companies operating across multiple jurisdictions.

In sum, Germany's implementation of GDPR demonstrates both the strengths of its constitutional privacy culture and the practical difficulties of federalism and resource constraints. While the legal framework is among the most advanced and citizen-oriented in the EU, the effectiveness of enforcement remains uneven.[87] This paradox—between strong principles and imperfect practice—highlights the central challenge of Germany's data

[83] A Roßnagel, A Pfitzmann and H-J Garstka, *Modernisierung des Datenschutzrechts: Gutachten im Auftrag des Bundesministeriums des Innern* (Bundesministerium des Innern 2001).
[84] M Albers, *Informationelle Selbstbestimmung* (Habilitation, Baden-Baden 2005).
[85] HA Wolff, S Brink and M Albers, *Datenschutzrecht in Bund und Ländern: Grundlagen, Bereichsspezifischer Datenschutz, BDSG: Kommentar* (2013).
[86] S Sädtler, 'Aktuelle Rechtsfragen des Datenschutzes und der Datensicherheit im Cloud Computing' (2013) 36(3) PIK – Praxis der Informationsverarbeitung und Kommunikation 165.
[87] A Roßnagel, 'Datenschutzfragen des Cloud Computing', in *Wolken über dem Rechtsstaat?* (Nomos Verlagsgesellschaft mbH & Co KG 2015) 19.

protection regime and provides a useful contrast with Italy's more centralized but less institutionally robust approach.

5. Comparison of Fines and Statistical Trends.

Since the entry into force of the General Data Protection Regulation (GDPR) in May 2018, national Data Protection Authorities (DPAs) across the European Union have actively enforced its provisions. The GDPR, adopted in 2016 and directly applicable in all Member States, introduced one of the most comprehensive data protection frameworks worldwide, with extraterritorial reach. It imposes strict obligations on organizations processing personal data, regardless of their geographic location, and establishes core principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.[88]

Non-compliance with these obligations may result in severe penalties of up to €20 million or 4% of a company's total annual global turnover, whichever is higher. Enforcement has therefore become not only a legal matter but also a reputational one: aligning with GDPR is increasingly perceived as a prerequisite for consumer trust and corporate credibility in global markets. The Regulation thus represents a new form of "regulatory export," shaping business practices beyond the EU's borders.[89]

Statistical analyses of enforcement actions reveal clear patterns. Across the EU, DPAs most frequently cite Articles 5 (general principles), 6 (lawfulness of processing), 12–13 (transparency and information obligations), and 32 (security of processing) when imposing sanctions. These articles address fundamental aspects of data protection and directly safeguard the rights of data subjects in the online environment. For example, Article 5 violations alone accounted for 33 out of 73 fines issued between May 2018 and September 2019, reflecting regulators' emphasis on foundational principles such as purpose limitation and data minimization.[90]

Enforcement has expanded dramatically over time. As of December 2023, DPAs across Europe had imposed more than 2,100 fines totaling over €4.4 billion. By March 2024, this figure had increased further, confirming GDPR's role as not merely symbolic legislation but as a robust enforcement mechanism with tangible economic impact.[91] The magnitude and scope of these penalties demonstrate that the GDPR has transformed data protection into a compliance

[88] CMS Law, GDPR Enforcement Tracker Report 2024 (CMS Legal Services 2024) https://www.enforcementtracker.com.
[89] A Andersson and S Borgernäs, 'Valuing Differential Privacy: Assessing the value of personal data anonymization solutions, specifically Differential Privacy-solutions, for companies in the mobility sector' (2022) (Dissertation). Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-319788.
[90] European Data Protection Board (EDPB), Annual Report 2022 (EDPB 2023) [https://edpb.europa.eu].
[91] E de Chazal, '20 Biggest GDPR Fines of All Time' (Skillcast, 29 August 2024) https://www.skillcast.com/blog/20-biggest-gdpr-fines; C Basunti, 'La (presunta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali' (2020) Contratto e Impresa, 860 ss.

priority for organizations across industries, from telecommunications and energy to social media and e-commerce.[92]

Italy has emerged as one of the most active jurisdictions in GDPR enforcement, ranking consistently among the top three EU Member States for the number and value of fines imposed. Since 2019, the Italian Data Protection Authority (Garante per la protezione dei dati personali) has significantly intensified its activity, particularly targeting the telecommunications and energy sectors, where unlawful telemarketing practices and inadequate consent management have been widespread.[93]

Several high-profile cases illustrate this trend. In 2020, TIM S.p.A. received a record fine of €27.8 million for extensive violations involving unsolicited promotional calls, including to individuals listed on the national "do-not-call" register, and for inadequate consent procedures. Vodafone Italia S.p.A. was fined €12.2 million the same year for unlawful use of personal data in telemarketing through fake numbers and inadequate security practices. More recently, in 2023, Enel Energia S.p.A. was sanctioned with the largest GDPR penalty ever imposed in Italy—€79.1 million—for failing to prevent unauthorized third-party telemarketing, coupled with insufficient data protection measures. Other notable cases include Edison Energia S.p.A. (€4.9m), Axpo Italia S.p.A. (€10m), and multiple sanctions against Eni Gas e Luce for unlawful advertising and inadequate data security.[94]

These enforcement actions reveal a clear pattern: the Garante has consistently prioritized consumer protection against aggressive telemarketing and unlawful marketing practices.[95] This reflects both the high volume of complaints filed by Italian citizens and the regulator's strategy of focusing on sectors with systemic non-compliance. At the same time, Italy has also imposed fines in areas such as financial services and utilities, underscoring the broad application of GDPR across industries.[96]

Statistical data confirms this rigorous approach. By March 2024, Italy had issued 389 fines totaling €237.3 million, placing it ahead of Germany in overall enforcement activity. Although many fines were relatively small, Italy's willingness to sanction both large corporations and smaller entities illustrates a comprehensive enforcement philosophy. Unlike Germany, which has focused on fewer but larger fines in cases of systemic violations, Italy's enforcement model is characterized by high frequency, sectoral concentration, and strong consumer orientation.

---

[92] K Salumaa-Lepik, N Nisu, 'Data Protection Chapter' in *Digital Development of the European Union: An Interdisciplinary Perspective* (Springer International Publishing 2023) 145.

[93] B Daigle and M Khan, *The Changing Tides of Data Protection Regulation and Enforcement in Europe* (Office of Industries, US International Trade Commission 2022); IA Caggiano, 'Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale' (2018) 1 Osservatorio del diritto civile e commerciale, 73; A Purpura, Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data*'* (2022) 4 in Jus civile 901.

[94] Garante per la protezione dei dati personali, Relazione annuale 2022 (Garante 2023) [https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9904277]; A Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale* (ESI 2019).

[95] J Wolff and N Atallah, 'Early GDPR penalties: Analysis of implementation and fines through May 2020' (2021) 11 Journal of Information Policy 63.

[96] G Gentile and O Lynskey, 'Deficient by design? The transnational enforcement of the GDPR' (2022) 71(4) International and Comparative Law Quarterly 799.

Germany has been another leading jurisdiction in GDPR enforcement, ranking third in Europe in terms of total fines issued. The German model reflects the country's federal structure, where 16 state Data Protection Authorities (DPAs) operate alongside the Federal Commissioner for Data Protection and Freedom of Information (BfDI). This decentralized approach has produced an assertive but fragmented enforcement landscape, with fines varying significantly between states such as Berlin, Hamburg, and Baden-Württemberg.[97]

Several high-profile cases illustrate Germany's strict stance. In 2020, the Hamburg DPA imposed a record fine of €35.5 million on H&M for excessive monitoring of employees, including unlawful collection of sensitive health data. Similarly, the Berlin DPA fined Deutsche Wohnen SE €14.5 million for retaining tenant data without legal grounds, a case that became symbolic of Germany's focus on data retention and purpose limitation. Other notable sanctions include notebooksbilliger.de (€10.4m) for unlawful video surveillance, 1&1 Telecom GmbH (€9.5m) for inadequate customer authentication, and AOK health insurance (€1.2m) for improper use of contest participants' data for advertising purposes. Smaller fines against banks, utilities, and real estate companies also demonstrate the breadth of German enforcement across industries.[98]

Despite these actions, critics note that German DPAs disclose only a limited number of cases, reducing transparency compared to Italy. Nevertheless, statistics show that Germany has imposed 202 fines totaling €55.6 million by March 2024. Roughly half of these fines involved violations of Article 6 GDPR (lack of a valid legal basis for processing), while about 17% were related to insufficient technical and organizational security measures under Article 32.[99] This aligns with Germany's emphasis on lawfulness of processing and data security, reflecting both its constitutional tradition of informational self-determination and its strong regulatory culture.[100]

The pattern of enforcement in Germany differs from that of Italy. While Italy's Garante focuses heavily on consumer complaints and unlawful telemarketing, German regulators target systemic issues such as employee monitoring, inadequate cybersecurity, and unlawful data retention. Fines in Germany are less frequent but often larger, and they tend to address structural compliance failures rather than individual consumer grievances. This distinction underscores the impact of Germany's federal enforcement model, which prioritizes long-term systemic compliance over high-volume sanctioning.

The enforcement of GDPR in Italy and Germany highlights two distinct but complementary models of regulatory practice within the European Union. Both

[97] İB Sayar, 'The administrative fines regime of the general data protection regulation and its impact' (2021) 3(1) Kişisel Verileri Koruma Dergisi 1.

[98] CMS Law, GDPR Enforcement Tracker Report 2024 (CMS Legal Services 2024) https://www.enforcementtracker.com.

[99] J Kaufmann et al., 'Germany: Another million euro fine under the GDPR in Germany – What does it tell us?' (26 November 2020) https://www.globalcompliancenews.com/2020/11/26/germany-another-million-euro-fine-under-the-gdpr-in-germany-what-does-it-tell-us16102020/.

[100] B Daigle and M Khan, The Changing Tides of Data Protection Regulation and Enforcement in Europe (Office of Industries, US International Trade Commission 2022).

countries rank among the leading jurisdictions in the number and value of fines, yet their approaches diverge in terms of focus, strategy, and institutional design.

Italy has adopted a high-frequency, consumer-oriented enforcement model. The Garante has issued a large number of fines—389 totaling over €237 million by March 2024—many targeting the telecommunications and energy sectors. Unlawful telemarketing, inadequate consent procedures, and aggressive marketing practices dominate the enforcement landscape. This reflects the high volume of citizen complaints in Italy and the regulator's strategy of addressing violations that directly affect consumers' everyday lives.[101] The Italian model is therefore characterized by broad coverage, sectoral concentration, and frequent sanctions, with penalties ranging from modest sums to record fines such as the €79.1 million sanction against Enel Energia in 2023.

Germany, by contrast, follows a lower-frequency, systemic enforcement model.[102] With 202 fines totaling €55.6 million by March 2024, German DPAs focus less on consumer grievances and more on structural compliance failures. High-profile cases, including H&M's €35.5 million fine for unlawful employee monitoring and Deutsche Wohnen's €14.5 million penalty for unlawful data retention, demonstrate Germany's emphasis on organizational accountability, data security, and the constitutional principle of informational self-determination. The federal system of 16 Länder authorities ensures broad oversight, but it also creates fragmentation and uneven enforcement practices across states.[103]

A comparative perspective reveals three key differences. First, volume versus severity: Italy imposes more fines across a wider range of organizations, while Germany issues fewer but often larger penalties targeting systemic problems. Second, focus of enforcement: Italy prioritizes consumer protection against telemarketing and marketing abuses, whereas Germany targets deeper institutional issues such as employee surveillance, cybersecurity, and data retention. Third, institutional structure: Italy's centralized Garante ensures consistency but faces challenges in handling a high volume of cases, while Germany's federal model provides broad coverage but at the cost of fragmented enforcement and reduced transparency.

Taken together, these patterns underscore that both Italy and Germany play a crucial role in shaping the EU's enforcement landscape. Italy illustrates the effectiveness of responsive, citizen-driven enforcement, while Germany highlights the importance of tackling systemic compliance failures. Their combined approaches demonstrate the flexibility of the GDPR framework, which allows for different national enforcement cultures while maintaining a shared European commitment to protecting data subjects' rights.

---

[101] G Alpa, 'La proprietà dei dati', in *Persona e mercato dei dati. Riflessioni sul GDPR* (CEDAM 2019) 11 ss.
[102] A Schmid and L Esser, 'Numbers and Figures – What Has Happened So Far, Expressed in Numbers' (undated) [https://cms.law/en/ita/publication/gdpr-enforcement-tracker-report/numbers-and-figures].
[103] C Ritzer and N Filkina, 'First multi-million GDPR fine in Germany: €14.5 million for not having a proper data retention schedule in place' (Data Protection Report, 11 November 2019) [https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/].

6. Conclusion.

The comparative analysis of GDPR enforcement in Italy and Germany demonstrates not only two distinct enforcement cultures but also two different conceptions of the role of data protection in contemporary society. Italy's centralized and consumer-oriented model illustrates how regulatory authorities can respond directly to citizens' grievances, particularly in areas such as telemarketing, unsolicited marketing campaigns, and aggressive commercial practices. Germany's federal and systemic model, by contrast, emphasizes structural compliance, organizational accountability, and the constitutional principle of informational self-determination. These divergences highlight the fact that while the GDPR was formally designed to harmonize protections at the European level, in practice it has become a flexible and adaptive framework, filtered through national traditions, legal cultures, and institutional capacities.

This flexibility represents both a strength and a weakness of the GDPR. On the one hand, it allows national supervisory authorities to tailor enforcement strategies to their citizens' needs and expectations, thereby reinforcing local legitimacy. On the other hand, it risks undermining the uniformity and predictability that the GDPR was meant to guarantee, leaving businesses facing legal uncertainty across jurisdictions and citizens experiencing uneven levels of protection. From a normative perspective, the Italian and German experiences also expose the unresolved tension between the inalienable character of personal data as a dimension of human dignity and its increasing commodification as an economic asset. The very fact that fines and sanctions are calculated as percentages of global corporate turnover illustrates how deeply data protection is now embedded within market dynamics. This raises a critical question: can the GDPR's promise of informational self-determination withstand the economic and technological pressures of the digital economy?

The challenge becomes even more acute in the context of artificial intelligence (AI). The rise of AI-driven data analytics, machine learning systems, and automated decision-making technologies fundamentally tests the adequacy of the current enforcement models in both Italy and Germany. AI systems rely on the massive collection and processing of personal data, including sensitive categories such as biometric identifiers, health records, and behavioral data. These practices directly intersect with GDPR principles such as transparency, proportionality, and purpose limitation. Yet, the opacity of AI algorithms, the difficulty of ensuring meaningful consent, and the challenges of guaranteeing explainability reveal structural gaps in the GDPR's regulatory design.

Italy, with its high-frequency and consumer-focused enforcement, will need to expand its institutional capacity not only to handle traditional privacy violations but also to oversee the complex risks posed by AI applications in areas such as automated marketing, profiling, and financial services. Germany, for its part, must address the fragmentation caused by its federal system to ensure that supervisory authorities apply coherent standards when confronting issues like employee monitoring, algorithmic bias, and cybersecurity vulnerabilities linked to AI technologies. At the European level,

closer cooperation between supervisory authorities, greater resources for technical expertise, and updated interpretative guidance from the European Data Protection Board will be indispensable to align AI governance[104] with the principles of the GDPR.[105]

Ultimately, the lesson is that compliance with the GDPR cannot remain a mere formal exercise of documentation and box-ticking. Strong oversight and significant sanctions are necessary, but they are not sufficient. What is required is the evolution of a genuine culture of accountability in which the values of the GDPR—transparency, fairness, proportionality, and respect for human dignity—are embedded into corporate governance, technological design, and public administration. Only by integrating these principles into the very architecture of AI systems and digital infrastructures can Europe ensure that the GDPR fulfills its dual mission: protecting fundamental rights while enabling a dynamic, innovative, and trustworthy digital economy. In this way, the GDPR will not only serve as a European legal standard but also as a global benchmark for reconciling the promises of artificial intelligence with the imperatives of privacy and human dignity.

[104] "The Artificial Intelligence Act (AI Act) was approved on 13 June 2024, published in the Official Journal of the European Union on 12 July 2024, and entered into force on 2 August 2024. In accordance with this Regulation, Law No. 132 of 23 September 2025, containing provisions and delegations to the Government in the field of artificial intelligence, was published in the Official Gazette No. 223 of 25 September 2025.".

[105] It is primarily based on the algorithmic analysis of data (personal and non-personal) for the construction of models functional to the adoption of decisions or to the making of predictions (so-called data mining). See A Giannopoulou, 'Algorithmic systems: the consent is in the detail?' (2020) 9(1) Internet Policy Review 2 ff. This mechanism entails the necessity of granting developers access to large quantities of data, since the greater the volume of data used, the more accurate and reliable the construction of the model—and thus the decision or prediction formulated by the system—will be. Conversely, AI systems based on inaccurate or insufficient datasets may generate erroneous or incomplete outputs that fail to take into account the specificities of certain categories of subjects. That said, the use of personal data for the development of AI systems falls within the notion of "processing" under art 4 GDPR and therefore entails compliance with the rules set out in data protection law, which are always safeguarded in all European legislative acts governing artificial intelligence. The development of artificial intelligence and its undeniable utility leads to questioning the adequacy of the current data protection framework in allowing the growth and implementation of AI, with particular reference to some fundamental principles of personal data processing contained in the GDPR, such as the principle of transparency (ex art 5(1)(a) GDPR), the right to explanation (art 22 GDPR), the principle of data minimisation (ex art 5(1)(c) GDPR), and the principle of purpose limitation (ex art 5(1)(b) GDPR). See E Troisi, 'AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla "intellegibilità" dell'algoritmo' (2019) EJPLT 47 ff.; V Fusco, 'Luci e ombre del GDPR nell'era dell'intelligenza artificiale' (2025) 1 Osservatorio del diritto civile e commerciale.