



Title: **GDPR: a blessing or a curse?**

24.11.2025

Written by: *Isabelle Neefs, Ine Pauwels*

Reading time: +/- 5 minutes

## Introduction

We use smartphones and smartwatches to track weight loss, map our runs, and monitor health signals such as heart rate, glucose levels and body temperature. As a result, healthcare professionals (HCP) can now track and treat their patients from a distance, drastically increasing access to a huge amount of personal data. Besides, HCPs create their own data too: consulting lab and scan results, sending emails, looking up reference values... All this information is accessible 24/7. The cloud is everywhere.

As a consequence, secure data storage becomes increasingly important. People are concerned about how their data is used, and they should be. What if they lose their smartphone? What if their medical record is hacked? Or if personal health data is shared with insurance companies? Protecting personal data against misuse is more relevant than ever.

## General Data Protection Regulation or GDPR?

Since 25 May 2018, every person, business, or organization managing personal data of European Union (EU) residents must be GDPR compliant. GDPR aims to give people in the EU more control about their own data and how it is used, for example the right to access and correct their personal data, the right to data portability, and the right to be forgotten or to withdraw consent.

## GDPR in healthcare?

Healthcare data is subject to higher protection standards because of its sensitive nature. As explicit consent for managing personal data is needed, many healthcare organizations fear the loss of valuable information or being unable to gather information at all. Still, the key to encourage people to share their personal data is to make it clear that they have control over what they share, and full transparency about how their data is managed, by whom and for what purpose.

## Legal Framework and Scope (GDPR Foundation)

To assess both benefits and costs, it is essential to outline the GDPR's core architecture. GDPR establishes a comprehensive framework for lawful processing (Article 6), conditions for consent (Article 7), data subject rights (Articles 12–22; e.g., access, rectification, erasure, data portability), and principles such as data minimization, purpose limitation, and accountability (Article 5). It tightens breach notification obligations (Articles 33–34) and imposes governance requirements (e.g., Records of Processing Activities, DPIAs) to promote transparency and accountability. Cross-border data transfers are governed by safeguards (Chapter 5, Articles 44–50), adequacy decisions, and instruments such as Standard Contractual Clauses. The GDPR's enforcement architecture features independent supervisory authorities and harmonized rules to ensure consistent application across member states (Recitals and Chapter VIII).

The legal framework secures several core aims: (a) strengthening individual rights and consent mechanisms; (b) promoting transparency through regulated notices and processing records; (c) expanding the scope of accountability via DPIAs and data protection by design; (d) enabling cross-border data flows while maintaining privacy protections; and (e) establishing a coordinated enforcement regime to deter noncompliance. While these provisions are generally lauded for clarifying expectations and elevating privacy standards, they also create ambiguity in certain areas (e.g., the precise boundaries of “legitimate interests” as a lawful basis) and impose administrative burdens that vary by organization size and sector (Regulation (EU) 2016/679; recitals).

## The GDPR as a Blessing

GDPR has been widely praised for several substantive gains. First, it strengthens privacy rights and user control. The rights to access, correct, delete, and port data empower individuals to challenge how organizations handle their information, contributing to enhanced consumer trust and perceived data stewardship. Second, it heightens transparency and accountability. Organizations must document data processing activities, assess privacy risks, and adopt privacy-by-design and privacy-by-default practices, which collectively raise the baseline for data governance. Third, GDPR promotes harmonization across the EU, reducing the “legal fragmentation” that previously complicated cross-border data flows and compliance. In practice, this harmonization supports smoother collaboration among multinational entities and helps align global privacy practices with EU standards, potentially shaping non-EU regimes through normative influence. Fourth, initial evidence suggests improvements in governance around data minimization, purpose limitation, and data breach notification, which can strengthen market trust and demonstrate a commitment to responsible data stewardship. These benefits are particularly salient for consumers who gain stronger recourse and clearer information about how their data is used (Regulation (EU) 2016/679; Recitals).

From an economic and innovation perspective, GDPR's blessing includes incentives for privacy-preserving technologies and governance-by-design approaches. The regulation's emphasis on risk-based, proportionate enforcement, and accountability mechanisms can spur investment in privacy-enhancing technologies, data governance platforms, and governance frameworks that accommodate data-driven research within ethical and legal boundaries. Taken together, these dynamics can yield an environment where privacy protections do not merely restrict activity but actively shape more trustworthy, transparent, and user-centric data ecosystems.

## The GDPR as a Curse

Despite its merits, GDPR imposes notable costs and constraints that some scholars and practitioners describe as burdensome or constraining. First, compliance costs are nontrivial, especially for small and medium-sized enterprises (SMEs) and startups with limited resources to implement robust privacy programs, conduct DPIAs, and maintain ongoing data governance. The administrative overhead—data inventory, documentation, consent management, DPIAs, and breach response—can divert resources from core activities and innovation. Second, interpretive ambiguity remains, particularly around “legitimate interests” as a basis for processing, consent fatigue, and the boundaries of consent in complex data ecosystems. Such ambiguities can lead to cautious or overly conservative data practices, potentially dampening experimentation and data-driven research. Third, there is concern about regulatory complexity and inconsistent enforcement. While the GDPR aims for harmonization, enforcement experiences vary across jurisdictions, and the risk of fragmentation persists if national regulators diverge in guidance, thresholds, or penalties. Fourth, some observers argue that GDPR may inadvertently hinder innovation by creating friction in legitimate data-sharing arrangements (e.g., medical research or AI development) or by privileging large incumbents with greater compliance bandwidth over nimble entrants. Finally, cross-border transfers still face ongoing governance challenges (e.g., after Schrems II, the adequacy of data transfer mechanisms depends on up-to-date, robust safeguards), which can introduce uncertainty and compliance risk for international collaborations (Schrems II; GDPR provisions on transfers).

## Stakeholders and Sectoral Variation

The impact of GDPR is not uniform across stakeholders or sectors. Consumers generally benefit from stronger rights and greater transparency, while SMEs and startups often bear higher relative costs, especially in early-stage data practices. Large multinationals may achieve economies of scale in compliance but also face ongoing expectations for robust accountability. Researchers and healthcare providers encounter both opportunities (clearer data governance expectations, potential for responsible data sharing) and constraints (restrictive consent frameworks, data minimization pressures). Sectoral variation is pronounced: in healthcare, stringent data protection norms must be balanced against the needs for timely patient data for care and research; in advertising, data flows and targeting practices face tighter restrictions but may drive innovations in privacy-preserving advertising models; in AI, data governance requirements intersect with model training data needs and data provenance concerns. Public-sector bodies encounter special obligations around transparency and accountability, but they also benefit from harmonized baseline rules for public data handling and interoperability.

## Case Studies and Empirical Evidence

A set of notable enforcement actions and regulatory developments illustrate GDPR’s real-world effects. The Schrems II decision (C-311/18) invalidated the EU-US Privacy Shield framework, highlighting the central importance of robust safeguards when transferring personal data outside the EU and shifting emphasis toward Standard Contractual Clauses (SCCs) and supplementary measures. Cross-border transfer practices became more complex, necessitating rigorous assessments of third-country data protection regimes. In practice, this has driven a wave of policy and operational adjustments, including more detailed data transfer

impact assessments, enhanced data localization considerations in some contexts, and greater attention to data lineage and provenance. Within the EU, data breach notification pressures have increased public and regulator awareness, contributing to improvements in incident response planning. Enforcement experiences show both compliance-driven improvements and residual concerns regarding enforcement consistency, penalties, and the time required for regulators to adjudicate complex cases.

**Policy Options and Best Practices** To preserve GDPR's privacy gains while reducing frictions for legitimate data activities, several policy options and best practices merit consideration. First, emphasize proportionality and risk-based enforcement, ensuring that compliance requirements align with an organization's size, data processing risk, and intended impact. Second, promote privacy by design and default across product lifecycles, including standard DPIA templates and sector-specific guidance to streamline adoption. Third, facilitate safe harbors or simplified processing regimes for clearly defined, low-risk activities, enabling experimentation while maintaining core protections. Fourth, provide clear guidance on lawful bases (especially legitimate interests) and consent in dynamic data ecosystems, reducing interpretive uncertainty for organizations and data subjects alike. Fifth, advance international cooperation to harmonize cross-border data transfer mechanisms, with ongoing alignment of SCCs, adequacy assessments, and cooperation frameworks among regulators. Finally, invest in capacity-building and guidance for SMEs, researchers, and startups, including accessible resources, templates, and training to lower the barrier to compliant data practices.

**Limitations, Counterarguments, and Gaps** No governance regime is without limitations. GDPR's emphasis on individual rights may interact with legitimate societal interests in data-driven innovation, philanthropy, and public health research in ways that require ongoing recalibration. Measurement challenges persist: evaluating GDPR's net impact on innovation, economic efficiency, and trust is complex and context-dependent. Some argue for more explicit exemptions or sector-specific guidance to reconcile privacy protections with critical research and development needs, particularly in health, AI, and climate analytics. The evolving technological landscape—edge computing, federated learning, and increasingly sophisticated data analytics—requires ongoing updates to guidance, enforcement practices, and international cooperation to ensure that rules remain effective without stifling beneficial innovation.

## How do we handle GDPR as a medical communications agency?

We monitor GDPR regulations and GDPR compliance remains one of our priorities, being an opportunity to further strengthen our commitment towards clients and partners. We have always respected the data privacy and protection rights of all our stakeholders, whether it concerns industry clients, medical experts or others. Only relevant data is collected and stored in a structured, transparent, secured and meaningful manner. By improving transparency with customers and raising awareness within the company about appropriate and secure data handling, we are ready for the future.

## More reading

1. <https://gdpr-info.eu/>
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 (General Data Protection Regulation). Official Journal L 119, 04/05/2016, p. 1–88.
3. Schrems II, C-311/18. (2020). Court of Justice of the European Union. [Decision related to data transfers and safeguards.]
4. Voigt, P., & Büsche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer.
5. European Data Protection Supervisor (EDPS). (2019). Privacy by design and data protection impact assessments: Practical guidance for organizations.
6. Information Commissioner's Office (ICO). (n.d.). Data protection practical guidance and case studies.
7. Additional scholarly and policy sources as you finalize your bibliography (e.g., articles on GDPR impact, enforcement trends, sector-specific analyses, and cross-border data transfer guidance).