# ARTICLE

## 5 YEARS LATER, WHAT IS THE ASSESSMENT OF THE GDPR?

Intellectual Property, Media, and Art Law | 30/05/23 | Florence Chafiol Alexandra Antalis

PROPRIÉTÉ INTELLECTUELLE

On May 25, 2018, the General Data Protection Regulation (GDPR) came into effect with ambitious objectives: to enhance citizens' control over their personal data, hold accountable the relevant actors, standardize the implementation of regulations across the European territory, and strengthen cooperation among authorities to legitimize regulation in this field. While it faced strong criticism at that time, with numerous organizations fearing it could hinder innovation and economic growth, it was also praised for the protection it was expected to provide individuals against the massive and sometimes uncontrolled processing of their data by internet giants.

Five years later, the GDPR appears to have fulfilled many of its missions but has also revealed its limitations.

- **A Surge in Complaints**

The highly publicized GDPR has succeeded in raising awareness among European citizens regarding the protection of their personal data. French citizens, in particular, have been notably active in this regard, with the CNIL recording over 12,000 complaints in 2022 [[1]], whereas its Irish counterpart received just under 3,000 [[2]]. The recent establishment by the CNIL of a reporting mechanism, allowing any individual to notify the authority of a GDPR violation they have become aware of [[3]], is likely to further increase the number of submissions in the coming years.

- **Increasingly Frequent Inspections and Record-Breaking Penalty Amounts**

The number of conducted inspections and subsequent measures taken [[4]], as well as the amount of imposed penalties, have significantly escalated over the years, compelling organizations to enhance their compliance out of fear of the financial repercussions and, more importantly, the reputational damage that a violation might expose them to. In total, European data protection authorities have imposed approximately 2.5 billion euros in fines over a span of five years. The CNIL stands out as one of the most proactive authorities, accounting for more than 500 million euros in fines since 2018.

However, these figures should be put into perspective as the majority of these amounts stem from sanctions against tech giants like GAFAM (making up nearly 93% in the case of France). While such penalties might seem substantial (for instance, CNIL fined Google 150 million euros in 2021), data protection authorities (particularly the Irish Data Protection Authority, responsible for overseeing most of the internet giants) have been criticized multiple times for being too lenient in limiting the potential sanctions' magnitude (which often constitutes only a tiny fraction of the penalized company's revenue, whereas the maximum amount can reach 4% of the global turnover). The European Data Protection Board has, on several occasions, issued decisions urging the Irish authority to revise upward the proposed sanction amounts within contentious proceedings. The issuance, on May 22, 2023, of a record-breaking fine of 1.2 billion euros against Meta [[5]] by the Irish authority reflects a likely trend of authorities being much more severe in the future.

- **Significant Cooperation among Regulatory Authorities**

European data protection authorities are increasingly collaborating effectively when GDPR violations involve cross-border data processing. More than 809 cooperation procedures have been implemented between 2018 and 2021, resulting in nearly 300 decisions being adopted [[6]]. While such cooperation undeniably promotes a harmonized interpretation and application of the GDPR across Europe, it still encounters challenges due to procedural differences between countries and lingering national legal specificities (for instance, concerning regulations related to health or commercial outreach), which curtail its scope.

- **Exploitation of Individuals' Rights**

By introducing new rights, requiring greater transparency from entities about their practices, and establishing stricter consent acquisition methods (such as the redesign of cookie banners on websites, necessitating users to click an "accept" button to consent to the use of trackers), the GDPR has unquestionably enhanced individuals' control over their data.

However, individuals, now well-informed about their rights, are increasingly prone to exploiting them for ancillary interests. Indeed, in recent years, there has been an exponential rise in requests for data access (under the basis of Article 15 of the GDPR), aimed at obtaining the disclosure of documents subsequently used as evidence in contentious proceedings,

particularly labor disputes. Faced with this misuse of the right to access, data controllers often find themselves in a delicate position, torn between their obligation to comply with the GDPR and their desire not to disclose elements that could incriminate them. The lack of pragmatism on the part of authorities in this regard, which mandates organizations to provide any data held regardless of the requester's motivation, is evident.

- **Discrepancies in Compliance**

While many large enterprises have achieved a significant level of maturity in GDPR compliance and allocate substantial resources for this purpose, the compliance level of SMEs and micro-enterprises often remains unsatisfactory. Less attuned to these matters and unable to allocate the financial and human resources necessary for implementing the numerous initiatives mandated by the GDPR, they frequently fall behind.

However, even within the most diligent companies, significant discrepancies in compliance are observed across different areas. Certain obligations are indeed challenging to adhere to, even for them, in light of economic realities. As an example, numerous organizations continue to engage vendors located in the United States and consequently transfer data to them, despite the invalidation of the Privacy Shield and the implications of the Schrems II ruling.

- **New Challenges**

The advancement of artificial intelligence (AI) presents unprecedented challenges and prompts us to question the adequacy and relevance of the current legal framework to effectively regulate the use of personal data by these new tools. The primary challenge for the GDPR, the forthcoming regulation on AI, and the authorities responsible for ensuring compliance in the coming years will be to strive towards shaping the development of privacy-respecting AI. This will involve appropriately and pragmatically guiding the stakeholders in this field.

---

[1] https://www.cnil.fr/fr/sanctions-et-mesures-correctrices-la-cnil-presente-le-bilan-2022-de-son-action-repressive

[2] Irish Data Protection Authority, 2022 Annual Report

[3] https://www.cnil.fr/fr/lanceurs-dalerte-adresser-une-alerte-la-cnil

[4] For instance, the CNIL conducted 345 inspections in 2022, resulting in 21 sanctions and 147 formal notices: https://www.cnil.fr/fr/sanctions-et-mesures-correctrices-la-cnil-presente-le-bilan-2022-de-son-action-repressive

[5] https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf - It's worth noting that while the Irish authority intended to impose a fine of 390 million euros on Meta, the EDPB (European Data Protection Board) determined that the penalty amount should fall within 20 to 100% of the applicable legal maximum, which is 4% of the total revenue of all entities within the Meta group.

[6] CNIL, 42nd Activity Report, 2021

---