



**FIVE YEARS UNDER
THE EU GDPR**

**BECOMING AN
ENFORCEMENT
SUCCESS**



Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grant-making, and convenings such as RightsCon, we fight for human rights in the digital age.

This paper is an Access Now publication. It is written by Estelle Massé. We would like to thank the Access Now team members who provided support, in particular Chiara Manfredini, Donna Wentworth, Sage Cheng, and Alexia Skok.

For more information, please visit:

<https://www.accessnow.org>

Contact: **Estelle Massé** | Senior Policy Analyst and Global Data Protection Lead **estelle@accessnow.org**

Published in May 2023

INTRODUCTION

The General Data Protection Regulation (GDPR) is a comprehensive data protection law designed to give individuals greater control over their personal information and to hold organisations accountable for the way they collect, use, and store personal information. When the law was adopted in 2018, the New York Times wrote "*G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*".¹ Five years later, this could finally be coming true.

Multiple challenges with the enforcement and application of the GDPR have put its success at risk. People have made use of their GDPR rights and filed complaints, but they often wait months, if not years, to see a remedy for data protection violations. Companies have become more aware of the need to consider privacy and data protection, but many have chosen a "risk-based approach" to compliance, deciding which GDPR measures they will or will not comply with in the hopes of avoiding hefty fines. These companies have not only put people's rights at risk, but in some cases may have gained an unfair advantage over companies that do make the effort to fully comply with the law.

The EU must ensure that the GDPR is a success to protect individuals' fundamental right to data protection and privacy, to ensure fairness in the digital economy, and to confirm its role as global leader in the protection of personal data. The GDPR is already a legislative success: now it needs to become an enforcement success story.

To pave the way for this success, the European Commission plans to propose a new law that aims to clarify and strengthen the GDPR's enforcement mechanism.² Access Now supports this initiative, which aims to harmonise the divergent national procedural rules that have led to delays and roadblocks in complaint resolution. This is what we asked for in our 2022 report on the enforcement of the GDPR.³ We commend the European Commission for moving ahead with the proposal and committing to making the GDPR a legislative and regulatory success.

The road ahead is still long and those undertaking to reform the enforcement mechanism must ensure that it is simplified, and that individuals and the NGOs that represent their rights remain empowered throughout the complaint resolution process.

In this report, we reflect on the importance of getting the enforcement right before providing concrete recommendations to improve the system.

¹ The New York Times, Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, 24 May 2018. <https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html>

² European Commission, *Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en

³ Access Now, *Four Years Under the EU GDPR, How to fix its enforcement*, July 2022. <https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf>

Five years in, the EU is opening a new chapter in the application of the GDPR, one where we hope to see its promise finally delivered.

I. DELIVERING ON THE PROMISES OF THE GDPR

The GDPR is an outstanding legislation, as measured by the impact it has already had at home and abroad:

- **Strengthened data protection rights:** The GDPR has bolstered data protection for individuals, giving them greater control over their personal data, including how it is used by organisations.
- **Increased data protection and privacy awareness:** The GDPR has greatly contributed to raising awareness about the importance of data protection and privacy among both individuals and organisations. Once an afterthought, these issues are now at the forefront of most technological debates.
- **Started a global data protection trend:** The GDPR has inspired many countries around the world to adopt or update data protection laws to provide individuals with stronger rights.

Yet, the potential of the GDPR is far from being realised.

At its core, the GDPR is a user-centric law that aims to put individuals back in control of their personal information, providing for a broad spectrum of users' rights, and a clear set of obligations for companies. Its biggest revolution was a new enforcement mechanism which allows data protection authorities (DPAs) to impose significant fines to discourage companies from breaching the law. In fact, since the GDPR became applicable in May 2018, DPAs across the European Economic Area (EEA) have levied 1,641 fines, for a total of € 2,787,143,873.⁴

Despite these results, there are growing concerns about how slowly and unevenly the GDPR has been enforced.⁵ We see significant hurdles in the resolution of complaints, in particular cross-border ones, due to discrepancies and difficulties in the way national DPAs work together. While the GDPR established a cooperation mechanism for DPAs to resolve cases together, most rely on their national administrative procedures to operate within this European system. This results in a fragmented and delayed application of the law.

A 2022 study conducted by the Data Protection Law Scholars Network for Access Now shows that, in practice, data subjects across the European Union do not have an equal right to lodge a complaint under the GDPR, as DPAs apply different and sometimes contradictory practices to handle complaints.⁶ This

⁴ Data from <https://www.enforcementtracker.com/?insights> as of 12 May 2023.

⁵ WIRED, Matt Burgess, *How GDPR Is Failing*, 23 May 2022. <https://www.wired.co.uk/article/gdpr-2022>

⁶ Data Protection Law Scholars Network (DPSN), *The right to lodge a data protection complaint: OK, but then what? An empirical study of current practices under the GDPR*, June 2022. <https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf>

happens despite the principle of primacy of EU law and the existing guidance from the European Data Protection Board (EDPB), which states that “an interpretation of a given provision must not undermine the effectiveness of EU law”.^{7 8}

The slow enforcement of the law has likely delayed an important expected effect of the GDPR: a sector-wide shift away from data-hungry corporate practices. While Big Tech companies have adopted GDPR-friendly language in their policies and communications, the prevailing business model remains centred around (excessive) data collection and exploitation. As a result, some companies may not even know which data they have, or where the information is stored. Yet it is highly personal information about us — our photos, messages, private moments — that they are gladly monetising, but evidently cannot figure out how to adequately protect. Case in point: an internal Facebook document obtained by *Motherboard* reveals that its engineers are concerned that the platform does not have an adequate level of control and explainability over how Facebook systems use data—even though Facebook representatives deny that there is a problem.⁹ Likewise, in February 2021, former Amazon employees told *POLITICO Europe* that the company has data security and protection problems that put “millions” of people’s data at risk.¹⁰ Later the same year, a joint investigation from *WIRED* and *Reveal* exposed serious flaws in the way Amazon handles customer data.¹¹

These companies are at the centre of some of the biggest GDPR cases. In fact, Amazon received the biggest GDPR fine to date when the Luxembourg DPA meted out a € 746 million penalty to the company in July 2021.¹² But with ongoing appeals, delayed decisions, and disagreements among regulators, companies have so far been able to absorb the cost of these penalties while their GDPR-violating practices and privacy-invasive business models remain mostly intact. Some are also choosing to meet only some of their GDPR obligations after doing an analysis of “risks” of fines in case of regulatory checks or of a complaint. In doing so, companies are treating the GDPR as an *a la carte* menu as they pick and choose which obligations to follow and which is less “risky” to ignore. With this risk-based approach to

⁷ See from EUR-Lex: “The principle of the primacy (also referred to as ‘precedence’ or ‘supremacy’) of European Union (EU) law is based on the idea that where a conflict arises between an aspect of EU law and an aspect of law in an EU Member State (national law), EU law will prevail. If this were not the case, Member States could simply allow their national laws to take precedence over primary or secondary EU legislation, and the pursuit of EU policies would become unworkable. The principle of the primacy of EU law has developed over time by means of the case law (jurisprudence) of the Court of Justice of the European Union.” The main rulings of the Court of Justice of the EU establishing this principle are *Van Gend en Loos v Nederlandse Administratie der Belastingen* (Case 26/62) and *Costa v ENEL* (Case 6/64).
<https://eur-lex.europa.eu/EN/legal-content/glossary/primacy-of-eu-law-precedence-supremacy.html>

⁸ European Data Protection Board, *Guidelines 02/2022 on the application of Article 60 GDPR, Version 1.0*, March 2022.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_en

⁹ VICE, Lorenzo Franceschi-Bicchierai, *Facebook Doesn’t Know What It Does With Your Data, Or Where It Goes: Leaked Document*, 26 April 2022. <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>

¹⁰ POLITICO Europe, Vincent Manancourt, ‘Millions of people’s data is at risk’ — Amazon insiders sound alarm over security, 24 February 2021. <https://www.politico.eu/article/data-at-risk-amazon-security-threat/>

¹¹ WIRED, Will Evans, *Amazon’s Dark Secret: It Has Failed to Protect Your Data*, 18 November 2021.

<https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/>

¹² POLITICO Europe, Laura Kayali and Vincent Manancourt, *Amazon fined €746M for violating privacy rules*, 30 July 2021.

<https://www.politico.eu/article/amazon-fined-e746m-for-violating-privacy-rules/>

compliance, companies are often denying us key rights and data security protections mandated under the law.¹³

Effective enforcement of the GDPR is necessary to course-correct these worrying practices. This will not only protect individuals' fundamental rights, but also help to ensure fairness in the digital economy.

II. THE ROAD TO SUCCESSFUL ENFORCEMENT OF THE GDPR

In early 2022, the Commission launched its plan to introduce a new Regulation to “harmonise some aspects of the administrative procedure” and “streamline cooperation between national data protection authorities when enforcing the General Data Protection Regulation in cross-border cases”.¹⁴ This represents an opportunity to streamline core aspects of the consistency and cooperation mechanisms developed under the GDPR. We particularly support the targeted effort to address the identified obstacles to enforcement while leaving the GDPR itself untouched, as its principles, rights, and obligations remain critical achievements for the protection of personal data and the free flow of information.

The objective of the upcoming legislation is twofold:

1. Improving cooperation between data protection authorities within the GDPR enforcement mechanism, and
2. Harmonising aspects of national procedural law to ensure clarity and strengthen enforcement of the law.

These objectives are complementary and must work together. That said, the second objective is particularly relevant for the realisation of the right to data protection in practice. When national procedures for enforcement are harmonised, individuals should have a more straightforward path to seek remedies for data protection violations.

To support this objective, it is critical that the European Commission’s proposal include clear deadlines for the different steps and processes that are part of complaint resolution. Experience with the current enforcement mechanism shows there is too much discretion for data protection authorities to interpret aspects of the complaint resolution process and set varying timeline for decisions.¹⁵ This has led to vast differences in the way GDPR complaints are “handled”, and significant delays for resolution.

¹³ Access Now, Fanny Hidvégi, Daniel Leufer, Estelle Massé, The EU should regulate AI on the basis of rights, not risks, 13 February 2021. <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/>

¹⁴ European Commission, *Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en

¹⁵ Data Protection Law Scholars Network (DPSN), *The right to lodge a data protection complaint: OK, but then what? An empirical study of current practices under the GDPR*, June 2022. <https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf>

As the Commission works to determine which aspects of administrative procedures should be harmonised and what elements of the cooperation mechanism between DPAs need further clarification, Access Now presents the following six recommendations to ensure that the system adequately protects and represents individuals' rights¹⁶:

RECOMMENDATIONS FOR THE UPCOMING REGULATION

1 The Regulation should apply to national and cross-border cases

Data protection is an exclusive competence of the EU. If the scope of the future Regulation were to be limited to cross-border procedures, it would effectively create two different procedures for the application of the same EU law and could potentially lead to an unequal right to remedy, good administration, and data protection for people in the EU.

2 The Regulation should set rules for the application of the following procedural rules for data protection complaints

- Right to lodge a complaint: Data subjects will be provided with clear information on how to exercise their right to lodge a complaint in their own language
- Admissibility and scope of complaints: DPAs shall review admissibility of complaints only one time based on criteria detailed in this Regulation
- Guarantee the fundamental right to good administration:
 - Defining who is a Party and the Right to be heard: Both the complainant and defendant are parties and have a right to be heard by the Lead Supervisory Authority (LSA), Concerned Supervisory Authorities (CSAs), and the EDPB
 - Access to documents: Both parties will have access to documents related to the case, as will all EDPB members
 - Decision: The LSA will always issue a reasoned decision

3 The Regulation should establish a detailed process and timeline for cooperation in cases under mechanisms detailed by Articles 60 and 65 of the GDPR

The Regulation shall establish the following processes for the handling and resolution of cross-border complaints:

Within maximum one month of receiving a cross-border complaint:

1. The Supervisory Authority assigns it a case number and case handler which will be notified to the

¹⁶ For more details about our recommendations, please read our answer to the European Commission Consultation: Access Now's feedback to the European Commission Consultation on "Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation", 22 March 2023.
<https://www.accessnow.org/wp-content/uploads/2023/03/Access-Now-GDPR-Procedural-Rules-Consultation-March-2023-.pdf>

complainant.

2. The SA logs the complaint and all related documents within the EDPB IT system to define and agree on: the main establishment and Lead Supervisory Authority, the list of Concerned Supervisory Authorities (CSAs), the admissibility, and the scope of the complaint. The decisions on these components will be notified to the complainant who shall have 15 days to object to any or all points, with the exception of the list of CSAs.
3. In case of disagreement between the LSA and the CSAs during this stage, the EDPB should decide on the matter within 15 days and present its decision to the LSA.

After completion of this process and within maximum six months of the receipt of complaint:

4. The LSA conducts and concludes investigations on the complaints within the scope defined with the CSAs. The CSAs may contribute to such investigation by providing documents and resources to the LSA. The LSA shall update the CSAs of progress at least every fortnight. The LSA shall share all documents linked to the investigation with the CSAs.
5. The LSA shall hear both parties equally at least once.
6. If the LSA fails to provide access to documents or inform the CSAs, the CSAs may bring up the matter to the EDPB who can issue decisions requiring the LSA to provide all information necessary for cooperation.

After the investigation and within maximum eight months of the receipt of the complaint:

7. The LSA shall prepare and finalise a draft decision and present it, as well as a summary of its findings to the CSAs and the EDPB. All documents shall be uploaded in the EDPB IT system.
8. The LSA can involve CSAs in the co-drafting of the draft decision and require assistance from relevant subgroups from the EDPB.

Final stages and possible dispute resolution:

9. After the presentation of the draft decision, the EDPB members have four weeks to issue reasoned objections to the LSA (as already established under the GDPR).
10. If no reasoned objections are issued the LSA has four weeks to issue a final decision.
11. Upon receipt of these objections, the LSA has one month to integrate comments to address them. Alternatively and within the same time frame, the LSA can decide to reject all or some objections by providing the EDPB secretariat with a summary of its draft decision and of the objections so that the case can move to the dispute resolution procedure foreseen under Article 65 of the GDPR.
12. The EDPB has to reach a final decision one month after receiving the case from the LSA, with the possibility of extending this process for another month or two depending on the complexity of the case. The EDPB shall hear both parties as part of this process.
13. The LSA has three weeks to adopt the final decision communicated by the EDPB.

Publication and communication of the decision:

14. Once a final decision is adopted, the EDPB, LSA, and CSA may publish the decision and it shall be added to the EPDB register. The decisions will be public and include the name of the parties.
15. The filing SA informs the complainant of the final decision. If the decision was reached in another language than the filing language, the CSA provides a summary of the decision upon notification in maximum 15 days after the decision was reached. A complete translation of the decision shall be provided to the complainant as soon as possible.

- | | |
|----------|---|
| 4 | The Regulation could introduce a “fast-track” process for the resolution of selected cases |
| 5 | The Regulation could require all members of the EDPB to appoint an EU Commissioner or point person tasked with cooperation |
| 6 | The Regulation should mandate the creation of a new IT system for case monitoring, cooperation, and reporting |

CONCLUSION

In today's data-driven world, the GDPR is a cornerstone legislation to ensure the protection of fundamental rights and fairness in the digital economy. However, as noted by the Advocate General Bobek of the Court of the Justice of the EU, without a strong enforcement mechanism, the GDPR measures risk becoming "paper tigers".¹⁷

The European Union became a leader in the regulation and protection of personal data when adopting the GDPR, and people are expecting and waiting for these rights to materialise. For the GDPR to be truly effective, it is essential to strengthen its enforcement and ensure that companies and public entities misusing data face real consequences.

The European Commission has the opportunity and responsibility to improve the current enforcement system. We support the launch initiative and efforts to improve cooperation between DPAs. We urge the Commission to equally ensure that the upcoming Regulation improves the enforcement mechanism for data subjects, in particular by effectively guaranteeing the complainant's right to good administration and providing clear deadlines for the complaint resolution process.

Access Now looks forward to working with the European Commission and the co-legislators to strengthen the enforcement of the General Data Protection Regulation and with it, effectively guaranteeing the right to data protection.

For more information, visit our page:

<https://www.accessnow.org/data-protection/>

¹⁷ Court of Justice of the European Union, Opinion of the Advocate General in Case C-645/19, 13 January 2021. Paragraph 122. <https://curia.europa.eu/juris/document/document.jsf?docid=236410&doclang=EN>