

FOUR YEARS UNDER THE EU GDPR

HOW TO FIX ITS ENFORCEMENT

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, 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 Fanny Hidvegi, 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 July 2022

INTRODUCTION

The European Union is a legislative superpower with a weak enforcement track record.

The latest demonstration of this reality is none other than one of the EU's flagship laws: the General Data Protection Regulation (GDPR).

Alarm bells over the unequal and slow enforcement of the GDPR have been ringing for a few years now. In December 2020, we said that: "the GDPR has been a legislative success but an enforcement failure".¹ This message, shared by many academics and civil society partners, has now reached the institutions.² In May 2022, the European Data Protection Supervisor gathered thousands of experts, from regulators to NGOs, consumer groups, and representatives of the private sector and the European Commission, to discuss a way forward for the enforcement of the GDPR.³

Few legislations have gone under the level of scrutiny than the GDPR since its adoption. Perhaps we all expected the GDPR to deliver on its promises too quickly. But, four years into the application of the GDPR, supporters of the legislation and thousands of people who filed complaints with their data protection authorities are waiting eagerly to see their data protection rights materialise. The road to data protection is paved with delays, uncertainty, and unequal access to remedy across the EU.⁴ Does this mean that it is time for a full legislative reform of the GDPR?

This option can seem tempting, in particular in the Brussels bubble, whose very existence relies on the legislative train never stopping. But if the issue lies with the (lack of) enforcement, will a change to the content of the GDPR make things better? It is unlikely. In fact, it may lead to a watering down of hard-fought protections for people's rights. A recast of the GDPR should be off the table, at least in the near future.

But then what? How do we deliver the benefits and promises of the GDPR in practice? These questions are at the center of this year's report: *Four years under the GDPR: how to fix its enforcement*. We first look into some of the causes of the problems with enforcement before proposing recommendations to the European Commission and data protection authorities to fix them.

I. WHAT IS WRONG WITH THE ENFORCEMENT OF THE GDPR?

Since the GDPR became applicable in May 2018, data protection authorities (DPAs) across the European Economic Area have levied a total of 1,132 fines for € 1,644,755,506.⁵ While fines are not and should not be the single metric to measure enforcement, this represents significant and deterrent work by the authorities.

¹ Access Now, *Three years under the GDPR, an implementation progress report*, May 2021.

<https://accessnow.org/GDPR-3-years>

² WIRED, Matt Burgess, *How GDPR Is Failing*, May 2022. <https://www.wired.com/story/gdpr-2022/>

³ European Data Protection Supervisor, *Effective enforcement in the digital world*, June 2022.

<https://www.edpsconference2022.eu/en>

⁴ 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://accessnow.org/gdpr-complaint-study>

⁵ Data from <https://www.enforcementtracker.com/?insights> as of 28 June 2022.

When we look into these numbers in detail, though, we start to see some of the issues with the enforcement of the legislation:

Slow resolution of cross-border cases: The resolution of cases related to large companies operating across several countries, including cases against so-called Big Tech companies, is taking a lot of time. Exact numbers concerning the resolution of cross-border complaints under Article 60 and 65 of the GDPR are not available.⁶ For 2021, the EDPB records a total number of 209 draft decisions under Article 60, which resulted in 141 final decisions, although not all of them led to fines or sanctions.⁷ The NGO noyb has filed around 50 cross-border cases under the GDPR, and as of June 2022, none of them are resolved.⁸

Many point to bottleneck issues with the functioning of the cooperation mechanism established by the GDPR, the one-stop-shop.⁹ The one-stop-shop mechanism is supposed to serve both people and companies. Through this system, an individual can bring a data protection complaint to the authority in the country where they live, even if the company against which they lodge the complaint is located in another country. Meanwhile, a company can designate a main establishment in the EU country where they take decisions about the use of data. The data protection authority of this country then becomes the “lead supervisory authority” for all complaints related to the company, regardless of where the complaint has been filed. The lead authority has to cooperate with other authorities where people may file complaints (the “concerned supervisory authorities”).

In practice, a few DPAs where large companies have set up their main establishment are responsible for dealing with the majority of cross-border cases: Ireland, Luxembourg, and to a lesser extent, the Netherlands.

Among those core DPAs for the enforcement of cross-border cases, the Irish Data Protection Commission (DPC) has faced the most intense pressure and the biggest intake of cases across the past four years.¹⁰ Since most large tech companies, including Meta, WhatsApp, TikTok, Google (mostly), and Microsoft are registered in Ireland, the DPC holds the key role of lead DPA in most high-profile cross-border cases under the GDPR. While the system assumes cooperation between DPAs, the Irish DPC has regularly failed to adequately involve its colleagues when resolving a case, or has involved them only at a late stage. This

⁶ Cross-border cases can be resolved through the one-stop-shop cooperation mechanism designed under Article 60 of the GDPR whereby a Lead Supervisory Authority (LSA) cooperates with Concerned Supervisory Authority (CSA) to agree on a decision. In case of disagreements between authorities that cannot be resolved, the case is escalated to the EDPB conflict-resolution mechanism under the procedure established in Article 65 of the GDPR. Under this process, the EDPB adopts a binding decision which is then communicated to relevant parties by the LSA. The EDPB maintains a register of final one-stop-shop decisions which gather most, but not all, cases due to a limitation on publication of cases in certain EU states. European Data Protection Board, *Final One Stop Shop Decisions*. https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

⁷ European Data Protection Board, *Letter to EDRI network NGOs*, June 2022. https://edpb.europa.eu/system/files/2022-06/20220614_edpb_reply_to_edri_letter.pdf

⁸ NOYB, *Statement on 4 Years of GDPR*, May 2022. <https://noyb.eu/en/statement-4-years-gdpr> and, NOYB, *Overview of noyb's GDPR complaints with DPAs*, 2022. https://noyb.eu/files/case_overview/case_table.html

⁹ Irish Times, Karlin Lillington, *Ireland is a 'GDPR bottleneck' that lets big tech off the hook*, September 2021. <https://www.irishtimes.com/business/technology/ireland-is-a-gdpr-bottleneck-that-lets-big-tech-off-the-hook-1.4686930>

¹⁰ Euractiv, Luca Bertuzzi, *Ireland's privacy watchdog accused of paralysing GDPR enforcement*, September 2021. <https://www.euractiv.com/section/data-protection/news/irelands-privacy-watchdog-accused-of-paralysing-gdpr-enforcement/>

means that the DPC, as lead DPA, may often decide on the scope or admissibility of a case on its own; or decide to prioritise its own investigation over cases NGOs or consumer groups have filed. This lack of cooperation and the sometimes isolated views of the Irish Data Protection Commission have created a significant political hurdle in what was already a complex legal system to apply.¹¹ If the Irish DPA's lone enforcer approach is not addressed, the whole cross-border enforcement system foreseen under the GDPR could fail.

Differences in national procedural laws and DPAs' national practices: The resolution of cross-border cases is often facing hurdles due to discrepancies and difficulties in the way DPAs work together. The GDPR has established a cooperation mechanism for DPAs to resolve cases together; however, most of them rely on their national procedure to operate within this European system. In practice, this means that DPAs leading on cases sometimes technically cannot share information on their draft decisions or investigations with colleagues. This happens despite the principle of primacy of EU law and the existence of guidance from the EDPB which indicates that “an interpretation of a given provision must not undermine the effectiveness of EU law”.¹² As with many other areas of law, we see a discrepancy between the way the GDPR should be applied in a harmonised manner and the prevalence of national procedures and interpretation.

The enforcement issues are not limited to the resolution of cases, however. They are present from the very moment someone wants to file a complaint. The Data Protection Law Scholars Network conducted a study for Access Now that shows that, in practice, data subjects across the EU do not have an equal right to lodge a complaint.¹³ The study found inconsistencies in the way DPAs deal with complaints. There are differences that span from whether and how a DPA will consider a complaint admissible, to the kind of information a DPA gives the data subjects, to how and where a subject can file a complaint, to whether and how the DPA will decide to proceed or fast-track a complaint, to what a subject can expect once the process is completed.

Faced with difficulties in filing cases with DPAs or obtaining a decision, people and NGOs are now considering directly turning to court to enforce the GDPR. Ironically, when the European Commission proposed the GDPR in 2012, it specifically sought to address the difficulties people have in getting remedy in relation to data protection violations via the courts. The Impact Assessment¹⁴ accompanying the proposed GDPR pointed out that:

¹¹ POLITICO Europe, Vincent Manancourt, ‘*Contrary to everything we believe in*’: Irish data watchdog lobbied for business-friendly GDPR, December 2021.

<https://www.politico.eu/article/irish-data-protection-commission-gdpr-lobby-business-friendly-general-data-protection-regulation/>

¹² 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

¹³ 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://accessnow.org/gdpr-complaint-study>

¹⁴ European Commission, *Impact Assessment accompanying the proposal for a Regulation 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 (General Data Protection Regulation)*, January 2012.

https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf

'(d)espite the fact that many cases where an individual is affected by an infringement of data protection rules also affect a considerable number of other individuals in a similar situation, in many Member States judicial remedies, while available, are very rarely pursued in practice'.

The European Commission added that there was:

'a general reluctance to bring an action to court, often related to the lack of information and the financial risk for the individual, when he/she is obliged to bear the costs of an unsuccessful claim for a judicial remedy, or when the damage is limited, e.g. in the case of unsolicited mails'.

As a result, the European Commission proposed a new enforcement model under the GDPR, which still guaranteed people's access to court, but offered a faster route to remedy through the data protection authorities. At least, on paper. It now seems that we have gone full circle on the enforcement options. While going to court may offer some resolutions, there is a risk of lack of harmonisation in the protection of rights across the EU as national courts do not have to cooperate. What is more, courts across the EU may not have the necessary expertise in the area of data protection.

II. RECOMMENDATIONS: FIXING THE ENFORCEMENT OF THE GDPR

To address the issues and challenges detailed in this report, Access Now has prepared the following recommendations:

RECOMMENDATIONS TO THE EUROPEAN COMMISSION

INTRODUCE NEW BINDING MEASURES TO CLARIFY THE ENFORCEMENT OF THE GDPR

We call on the European Commission to introduce a complementary legislative measure to the GDPR:

- To address the **slow resolution of cross-border cases and bottlenecks created by the one-stop-shop**. The Commission could consider granting **more power to EDPB** for large cross-border cases.
- To address **differences in national procedural laws**. The Commission could **give binding force to EDPB guidance and guidelines**, clarifying key definitions, admissibility criteria, and how the cooperation mechanism should work in practice, and could harmonise practices for data subjects' right to lodge a complaint and grant EU-wide right to be heard.

These changes should be done in a separate legislative tool. We call on the European Commission not to propose a recast of the GDPR and to respect and uphold its core principles and rights.

RECOMMENDATIONS TO THE NATIONAL DATA PROTECTION AUTHORITIES

CHALLENGE MAIN ESTABLISHMENT DETERMINATION FOR BIG TECH

The use of the one-stop-shop mechanism should be limited to companies that truly have a "main establishment" in the European Union. Often, EU entities of large tech companies do not truly have a place of central administration in the EU and/or they do not decide alone on the processing of data happening on their services. Instead, they do so together with headquarters located outside the European Union. This would suggest that these companies do not have a "main establishment" in the sense of the GDPR and therefore cannot use the one-stop-shop. This means that potentially all, and not just one DPA, could take on cross-border cases against said companies.

There might also be situations where a company only has a main establishment for some but not all processing activities.

We encourage DPAs to verify if and when companies have a main establishment to help address the **slow resolution of cross-border cases and bottleneck created by the one-stop-shop.**

INCREASE NUMBER OF JOINT INVESTIGATIONS

We encourage DPAs to work together and launch joint investigations to address systemic violations of data protection and cross-border data protection matters.

RECOMMENDATIONS TO NATIONAL GOVERNMENTS

INCREASE RESOURCES FOR DPAs

For DPAs to function properly and be able to address a large number of complaints, **governments across the EU must increase the financial and human resources allocated to them**, including support for technical staff.

GUARANTEE DPAs' INDEPENDENCE

Governments must **guarantee the independence of DPAs**, both in statutes and financially.

CONCLUSION: WHY IT MATTERS TO MAKE THE GDPR WORK

In 2018, in preparation for the entry into application of the GDPR, the European Commission said:

“On 25 May, a new single set of data protection rules will enter into effect across the EU. The new framework will bring significant benefits to individuals, companies, public administrations and other organisations alike. It is also an opportunity for the EU to become a global leader in personal

*data protection. **But the reform can only succeed if all those involved embrace their obligations and their rights.***¹⁵ (emphasis added).

Four years into the application of the law, there are multiple challenges to its enforcement that put its success at risk. In the meantime, companies that have so far failed to comply with the updated rules under the GDPR may have an unfair advantage over those that are in compliance, even as they put people's rights at risk. The “business as usual” or “bare minimum compliance” attitude is harmful for the digital economy and human rights alike. On a political level, if the EU’s promises do not materialise, it could cost the EU its global leadership on data protection in the digital age.

We all have a role to play in making the GDPR a success, individually and collectively. That includes NGOs, Data Protection Authorities, and the European Data Protection Board. We still do not have a full picture of the successes and issues of the GDPR enforcement model, which is why additional research will be needed. As noted by the Data Protection Law Scholars Network in the study conducted for Access Now:

*“to better understand the implementation and enforcement of the GDPR it is imperative to mobilise knowledge of both EU and national laws. This study clearly demonstrates how the procedures applicable at national level have the capacity to hinder the effective protection of EU Charter rights. These procedures therefore require further scrutiny which will necessarily touch upon a variety of fields of national law while also requiring attentiveness to the many languages and contexts in which the GDPR is applied in practice. This will demand additional efforts and cooperation from researchers, but it is scientifically valuable work.”*¹⁶

On the challenges we already know and which are highlighted in this report, we particularly need the European Commission to step in and course-correct.

We continue to believe in the potential of the GDPR and we stand ready to support data protection authorities, the European Commission and legislators in this next phase of the application of the law.

For more information, visit our Data Protection page:

accessnow.org/issue/data-protection

¹⁵ European Commission, *Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*, January 2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043>

¹⁶ 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://accessnow.org/gdpr-complaint-study>