accessnow

accessnow.org

THREE YEARS UNDER THE EU GDPR

AN IMPLEMENTATION PROGRESS REPORT

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 report 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 Daniel Leufer, Donna Wentworth, Sage Cheng, Juliana Castro, 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**

EXECUTIVE SUMMARY | MAY 2021

It has been three years since the General Data Protection Regulation (GDPR) entered into application. The hopes and expectations raised by this flagship legislation are turning into frustration over the slow enforcement of the law. The sweeping privacy improvements that people were promised have yet to materialise: many complaints remain unaddressed, data protection violations routinely make headlines, and most Big Tech companies are resisting changes to their data harvesting business models.

The GDPR is described as "one of the European Union's greatest achievements in recent years".[1] It is viewed as a legislative success and has become a global model for regulation to protect personal data. All of this will mean very little, however, if the law fails to deliver tangible improvements for people's lives by protecting their rights to privacy and data protection. In our second GDPR progress report, published in May 2020, we wrote: "The GDPR will be as strong as its weakest link and we cannot let that weak link be the enforcement process and the bodies in charge of representing our rights. Even the best law in the world will bring little benefit if it is not applied".[2]

The GDPR is still in its infancy and it is far too early to discuss any revision of the legislation given that many of its tools are not yet being used. That said, the past three years hold important lessons that decision-makers and regulators can leverage to improve the situation.

In this report, we start by looking at the facts and figures on the GDPR to evaluate the enforcement action of data protection authorities (DPAs). From May 2018 to March 2021, DPAs levied **596 fines** and sanctions for a total of €**278,549,188**. Data on the use of fines shows a huge discrepancy across member states in how DPAs are using their powers. The most active DPA (Spain) has levied **223 fines** since May 2018 while the least active DPAs (Luxembourg and Slovenia) have yet to issue a single fine.[3] In addition, several DPAs across Europe are seeing their fines being cut after those penalized file challenges and appeals or through payment schemes that allow fines to be reduced.

---

[1] European Data Protection Supervisor, *The History of the General Data Protection Regulation.* https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[2] Access Now, *Two years under the EU GDPR*, 2020. https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf

[3] In a letter published by POLITICO Europe, Xavier Better, Luxembourg's Prime Minister and Digital Minister, indicates that the DPA has issued "two fines" but at the time of publication, there is no information available of these sanctions on the DPA's site. https://pro.politico.eu/news/politico-pro-cyber-insights-luxembourg-responds-budapest-convention-microsofts-eu-bet

While the total number of fines continues to increase, a huge number of complaints from individuals remain unaddressed and the resolution of cross-border cases is painfully slow. We therefore decided to **listen to what the DPAs — those at the centre of GDPR enforcement — have to say,** so we could better understand the issues they face and propose appropriate solutions. We read DPAs' annual reports, studied their answers to a detailed 2020 European Data Protection Board (EDPB) survey on the implementation of the GDPR, heard them speak about their experiences at multiple events, and analysed the minutes of the EDPB meetings.[4]

We have found that the majority of DPAs are experiencing significant problems with the application of the so-called one-stop-shop mechanism, a key tool for the enforcement of the GDPR in cross-border cases. **DPAs have identified four main issues with the operationalisation of the one-stop-shop** and **cooperation between authorities**:

(1) use of inadequate communications tools,
(2) incompatibility of different national procedures,
(3) lengthiness of the process for cooperating, and
(4) difficulties in identifying who is in charge of cases.

In addition to these operational difficulties, the work of DPAs is hindered by **insufficient financial and staff resources**. Our 2020 report largely focused on this issue but it has not been addressed by the EU and its member states.

Finally, frustration over the ponderous enforcement of the GDPR has led to disagreements among DPAs and the tension has translated into public fights. Cooperation between DPAs is at the centre of the GDPR enforcement mechanism, so it is critical that DPAs are able to communicate openly and have clear processes in place to avoid these conflicts. In the final section of this report, **we provide recommendations to the European Commission, DPAs, and member states to address the shortcomings we have identified**.

Getting the enforcement of the GDPR right is essential for safeguarding people's rights to privacy and data protection. The law is a flagship model for regulation which means the EU must carefully consider lessons from its application and the functioning of its enforcement mechanisms as it develops future legislative instruments, including the proposed Digital Services Act, Data Governance Act, and Artificial Intelligence Regulation.

[4] See for instance: European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

TABLE OF CONTENTS

INTRODUCTION

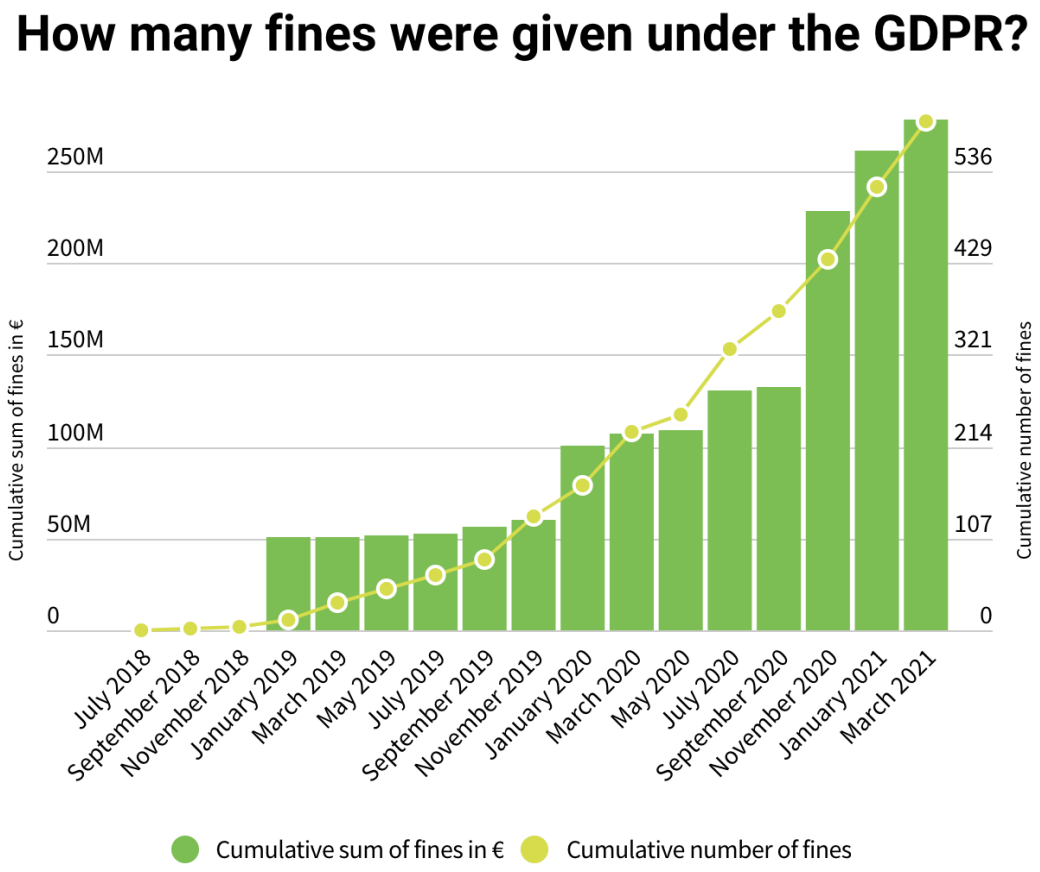
Three years ago, the EU General Data Protection Regulation became applicable. We could use one word to describe each of these first three years: hope, crisis, and frustration. During its first year, the GDPR increased awareness of data protection rights among citizens, governments, and businesses. We were hopeful and eager to see the GDPR bring about positive changes, making data protection a reality for people and spurring the development of privacy-friendly business practices. The second year proved to be a year full of challenges for the GDPR, with administrative, political, and global health crises impacting the ability of DPAs to enforce the law. This third year has been a year of frustration over the slow enforcement of the law. This situation has sparked criticism from the public, lawmakers, and even the regulators themselves.

In this report, we look at the data on GDPR enforcement to evaluate the actions of data protection authorities. We then analyse the DPAs' own experience with the GDPR with the aim of providing actionable recommendations to improve the application of the law.

I. ENFORCING THE GDPR: THREE YEARS IN NUMBERS

THIS IS FINE(S)

From May 2018 to March 2021, data protection authorities levied **596 fines** and sanctions.[5] They applied **364** of these fines between March 2020 and March 2021. Data from the last three years compiled in the graphic below show a steady increase in the number of fines.

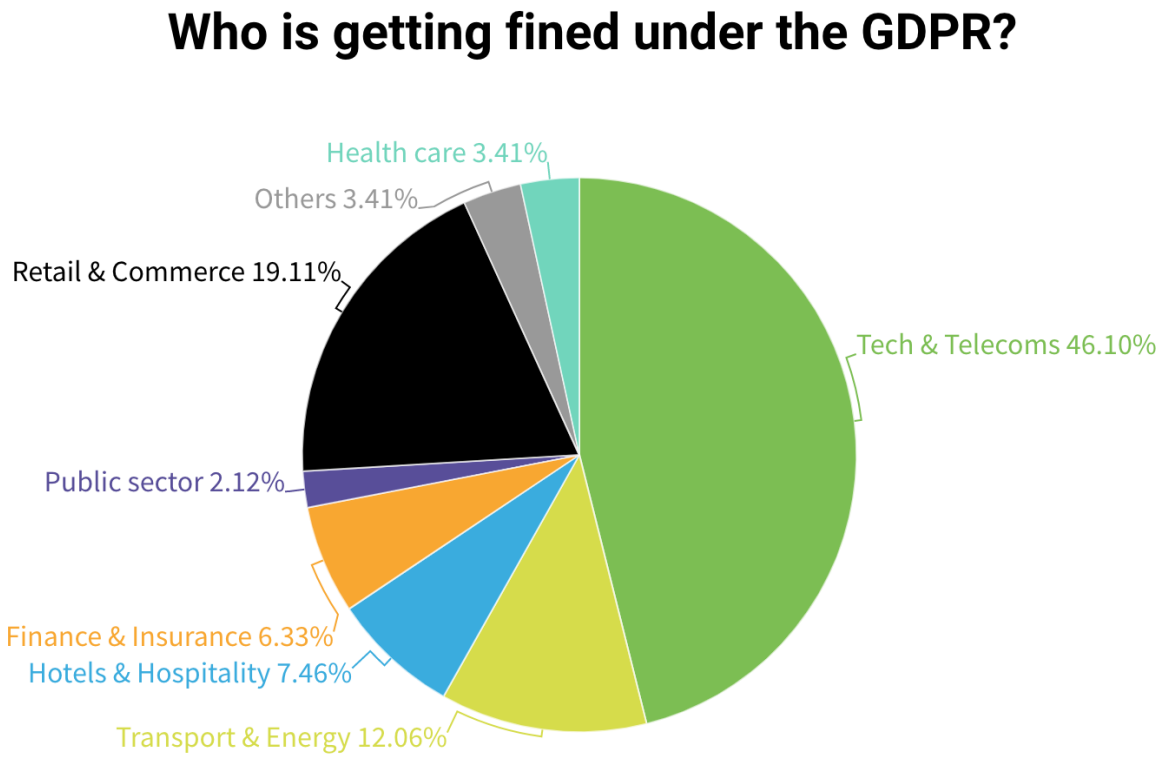


Source: https://www.enforcementtracker.com/?insights / Interact with this chart

Nearly half of all GDPR fines are being levied against **tech companies and telecommunications operators (46.1%)**. This result can be explained by the large number of individual complaints filed against them. In addition, these companies are known for their extensive use or access to individuals' personal data, which means that

[5] Data from May 2018 to 12 May 2021. All data on fines is from: CMS, *GDPR enforcement tracker*, 2020. https://www.enforcementtracker.com/?insights

supervisory authorities are expected to monitor their activities closely. Having said that, the GDPR applies to all sectors and DPAs have imposed fines on both public and private entities across industries. They have imposed a significant number on the **retail industry (19%)** as well as on companies from the **transport and energy sectors (12%)**.



Source: https://www.enforcementtracker.com/?insights / Interact with this chart

Spain has issued the **highest number of fines, with 223** so far, followed by Italy, with 73, and Romania, with 56. Over the past three years, Spain has consistently been the leading DPA in terms of the number of fines levied. Spain's total number of fines represents an average of **six fines per month** since May 2018. Six is also the total number of fines the DPAs from Ireland and Slovakia have issued since the GDPR became applicable. That is a low number, but these two DPAs are not at the bottom of the list for fines. Over the past three years, Malta has issued one fine, Croatia two, and Portugal four followed by Estonia, Latvia, Lithuania, and Finland, which have each issued five. **Luxembourg and Slovenia have the sad distinction of not having issued a single fine**.[6] Worse still, Slovenia — which will hold the presidency of the EU from July 2021 — has not fully implemented the GDPR into its national law.

[6] In a letter published by *POLITICO Europe*, Xavier Better, Luxembourg's Prime Minister and Digital Minister, indicates that the DPA has issued "two fines" but at the time of publication, there is no information available of these sanctions on the DPA's site. https://pro.politico.eu/news/politico-pro-cyber-insights-luxembourg-responds-budapest-convention-microsofts-eu-bet

The Spanish DPA — AEPD — has fined a large number of organisations in the country from many sectors, including banks, airlines, pub owners, and tech companies. Spain's active enforcement of the GDPR is noteworthy, but it has also attracted some criticism, with some questioning the AEPD's approach, including when issuing several fines against the same companies. For instance, it has fined the telecom operator Vodafone España no less than 29 times. *Global Data Review* reported on this "curious saga" noting, "No other company has received such a high number of GDPR fines, and no other regulator has enforced in this manner. What's more, the first penalties were imposed well over a year ago, suggesting a pattern of continued breaches of the law over an extended period".[7] It is unclear why the DPA would repeatedly issue fines to Vodafone instead of opening a broad investigation into the company's data practices, which appear to be problematic.

When it comes to the size of fines, **Italy has imposed the largest total amount,** at more than **€76 million** to date. **France comes in second place with nearly €55 million in fines**, although most of that total comes from a single €51 million fine imposed on Google.[8] **Germany closes out the top three with just over €49 million**.

Last year, the **United Kingdom was heading this ranking with a projected amount of** more than **€315 million** in fines. However, two of the biggest fines announced in the UK, against British Airways (€204 million) and Marriott International (€110 million), were **delayed** and then **significantly reduced**. The UK DPA — the ICO — **issued the revised fines in October 2020**: €22 million for British Airways (BA) and €20 million for Marriott International.[9] The final fine for BA represents only 10% of the originally announced fine. The ICO cited the difficulties that both the airline and hospitality company have faced during the COVID-19 pandemic to justify this drastic reduction in the amount of the fine.[10] With these revised figures, **the UK — which is no longer part of the EU but continues to apply the GDPR, for now — has levied** just over **€44 million in fines.**

Several DPAs across Europe have had their fines cut. *Global Data Review* reported that "Nearly €80 million in fines levied by European data protection authorities have been

[7] Sam Clark, Global Data Review. *The curious saga of Vodafone Spain*, 2020.
https://globaldatareview.com/data-privacy/the-curious-saga-of-vodafone-spain
[8] CNIL, *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, 2019.
https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
[9] ICO, *ICO fines British Airways £20m for data breach affecting more than 400,000 customers,* 2020.
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/ and;
ICO, *ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure*, 2020.
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/
[10] Ingrid Lunden, Tech Crunch, *UK's ICO reduces British Airways data breach fine to £20M, after originally setting it at £184M*, 2020.
https://techcrunch.com/2020/10/16/uks-ico-downgrades-british-airways-data-breach-fine-to-20m-after-originally-setting-it-at-184m/

dropped".[11] In Italy, the DPA offers an early payment scheme, which allows companies to pay half the fine originally imposed if they waive their right to appeal. To date, at least five companies have used this scheme to reduce their fines.[12] In Germany and Sweden, other fines were reduced after being challenged or appealed. Some companies have even had their fines completely overturned, including an €18 million fine against Austrian Post and a €14.5 million fine against Deutsche Wohnen, a German property company.[13] All fines that have been challenged or overturned came under dispute over procedure, and there are rarely challenges to the fact that a data protection violation occurred.

THE STRUGGLE IS REAL

Data on the use of fines for the enforcement of the GDPR shows that there is a huge discrepancy in how DPAs are using their powers. While the number of fines continues to increase, a huge number of complaints from individuals are unaddressed and the resolution of cross-borders cases is painfully slow.

Fines are obviously not the only metrics to evaluate enforcement of the GDPR. DPAs across Europe regularly indicate that a significant number of complaints are "resolved" amicably, with the simple issuance of a warning, or without fines needing to be imposed.[14] In such cases, more transparency from the DPA on the resolution of complaints is necessary, as it is often difficult to understand how an authority reaches a decision.

DPAs have imposed other important punitive sanctions and enforcement actions since May 2018. In April 2021, the Portuguese DPA — CNPD — ordered transfers of census data to the United States to stop as an "adequate level of data protection" cannot be guaranteed in the country.[15] Yet, the difficulties DPAs experienced in issuing and applying their fines is worrying.

---

[11] Sam Clark, Global Data Review, *European data enforcers can't make their fines stick*, 2021.
https://globaldatareview.com/data-privacy/european-data-enforcers-cant-make-their-fines-stick
[12] Vodafone Italia, Eni Gas e Luce, TIM, Wind Tre and Fastweb.
[13] Sam Clark, Global Data Review, *€18 million GDPR fine overturned,* 2020.
https://globaldatareview.com/data-privacy/eu18-million-gdpr-fine-overturned and;
Sam Clark, Global Data Review, *Multimillion-euro German fine overturned, but fight continues,* 2021.
https://globaldatareview.com/data-privacy/multimillion-euro-german-fine-overturned-fight-continues
[14] See for instance: Irish Data Protection Commission, *Annual report 2020.*
https://www.dataprotection.ie/sites/default/files/uploads/2021-02/DPC%202020%20Annual%20Report%20%28English%29.pdf
[15] CNPD, *CENSOS 2021: CNPD SUSPENDE FLUXOS PARA OS EUA*, 2021.
https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/

The slow resolution of complaints and absence of fines, in particular in cases being handled by the Irish DPA, the DPC, has come under heavy criticism. Many large tech companies have declared their main establishment in Ireland, so the DPC has become the lead authority in a significant number of high-profile cases that impact the rights of individuals all across the EU. This is the case for most complaints involving Google, Facebook, Twitter, WhatsApp, or Microsoft. So far, the DPC has reached a final decision in only four of 196 cross-border cases in which it is the lead supervisory authority, and a couple of other cases are currently being debated at the European Data Protection Board.[16] The complexity and slow handling of cases in Ireland has been an issue since the first day the GDPR entered into application and the DPC itself has acknowledged the problem.[17]

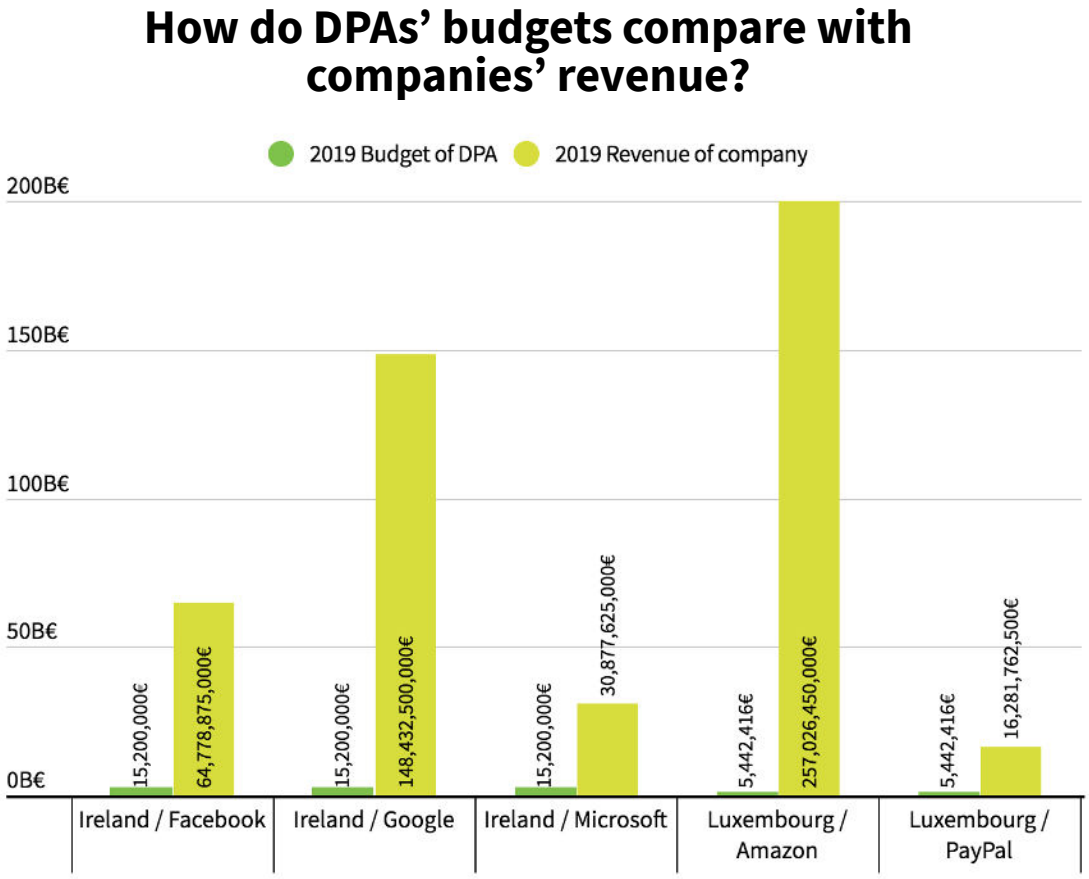
Against this background, in March 2021, the European Parliament and the German Federal Data Protection Authority raised serious concerns over a "lack of enforcement" of the GDPR by several DPAs, including the Irish DPC.[18] The DPC rejected the criticism and pointed to similar deficiencies in enforcement in other EU countries, including Germany. In fact, several fines imposed in Germany have been overturned or reduced after appeal.[19] This public fight between DPAs is a sign of the tension that exists between authorities which are supposed to work together within the European Data Protection Board to bring the GDPR to life.

The design of the GDPR gives a key role to Ireland in enforcing the law. It is therefore understandable that so much attention is directed at the DPC. Yet, there are several issues in the application of the GDPR that are not limited to Ireland. In fact, every data protection authority across the EU has been struggling with enforcing the GDPR. Nearly all do not have enough budget and resources to properly oversee the application of the GDPR and a majority report issues with the functioning of the cooperation mechanism.

Even if a number of authorities have received additional budget and staff since 2018, it is far from sufficient for matching up against large tech companies that can spend a virtually endless amount of resources to challenge DPA decisions and delay procedures. The

[16] Derek Scally, The Irish Times, *Irish data regulator sparks row with EU colleagues on Facebook oversight*, 2021. https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065
[17] Charlie Taylor, The Irish Times, *DPC rejects criticism of its regulation of big tech companies,* 2021. https://www.irishtimes.com/business/technology/dpc-rejects-criticism-of-its-regulation-of-big-tech-companies-1.4549370
[18] Derek Scally, The Irish Times, *Irish data regulator sparks row with EU colleagues on Facebook oversight*, 2021. https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065
[19] Vincent Manancourt, POLITICO Europe, *Germany struggles to walk the talk on privacy,* 2021. https://pro.politico.eu/news/133479

graphic below illustrates the disparity of resources between data protection authorities and the companies they are supposed to keep in check.



Consider Ireland, for example, where the revenue of some of the companies the Irish DPC is monitoring is higher than the country's Gross Domestic Product. In its most recent pre-budget submissions, the Irish DPC has described itself as being "acutely strained" when facing the "disproportionate resources" of tech firms and as lacking a "fit-for-purpose management and organisation structure" because it has not received the increased funding necessary to facilitate its new role as the de facto regulator of the "internet industry" across Europe.[20] The DPC is however about to receive additional staff to help deal with the large number of cases falling under its jurisdiction. *Global Data Review* reports that the DPC will bring in 71 new staff in 2021. This "will bring the watchdog's total employees to 220, up from around 150, equating to an approximately 46% increase".[21] While positive, the ressources gap between the DPC and the companies it

[20] Ken Foxe, The Irish Times, *Data Protection Commission 'acutely strained' by big tech cases*, 2021. https://www.irishtimes.com/business/technology/data-protection-commission-acutely-strained-by-big-tech-cases-1.4457683
[21] Sam Clark, Global Data Review, *Exclusive: Strained Irish data regulator gets big staff boost,* 2021. https://globaldatareview.com/data-privacy/exclusive-strained-irish-data-regulator-gets-big-staff-boost

oversees remains enormous. The situation is not any better for the Luxembourg DPA — the CNPD — which is responsible for handling cases related to the e-commerce and tech giant Amazon. What is more, *The New York Times* reported that in 2020, Amazon paid no corporate tax to Luxembourg, where the company has its European headquarters. The company had a record-breaking year revenue of €44 billion in Europe but reported a loss of €1.2 billion to the Luxembourg authorities.[22] *The New York Times* notes that: "The loss, which was due in part to discounts, advertising and the cost of hiring new employees, also meant the company received €56 million in tax credits that it could use to offset future tax bills when it makes a profit, according to the filing, released in March".

Finally, beyond insufficient resources and disagreements among DPAs, the implementation of the one-stop-shop mechanism is proving to be perhaps one of the biggest hurdles in the enforcement of the GDPR. In fact, some DPAs, including the French CNIL, have increased their enforcement actions under the ePrivacy Directive, perhaps to avoid having to use the one-stop-shop. Under this legislation linked to the GDPR, authorities can act independently to apply sanctions and do not have to rely on cooperation with other DPAs. In December 2020, the CNIL fined Google and Amazon for €100 and €35 million respectively for privacy violations.[23] In the decisions, the CNIL specifically recalls it competence:

> *In its decision, the restricted committee recalled that the CNIL is materially competent to control and sanction cookies placed by the company on the computers of users living in France. Thus, it emphasized that the cooperation mechanism provided for by the GDPR ("one-stop shop" mechanism) was not intended to apply in this procedure since the operations related to the use of cookies fall under the "ePrivacy" directive, transposed in Article 82 of the French Data Protection Act.*

While it is encouraging to see DPAs looking for solutions to enforce privacy and data protection rights, the current situation is not sustainable.

[22] Jenny Gross, Adam Satariano, The New York Times, *Amazon Had a Big Year, but Paid No Tax to Luxembourg*, 2021. https://www.nytimes.com/2021/05/04/business/amazon-corporate-tax.html

[23] CNIL, *Cookies: financial penalty of 35 million euros imposed on the company AMAZON EUROPE CORE*, 2020. https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core and; CNIL, *Cookies: financial penalties of 60 million euros against the company GOOGLE LLC and of 40 million euros against the company GOOGLE IRELAND LIMITED*, 2020. https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland

I. THE ONE-STOP-SHOP: IS THE COOPERATION MECHANISM BROKEN?

HOW IT STARTED

The GDPR establishes a complex mechanism for cooperation and consistency in the application of the law, which should support the resolution of cross-border investigations.

This system is based on the so-called one-stop-shop mechanism which 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 authority" for all complaints related to the company, regardless of where the complaint has been filed. This means that the lead authority has to cooperate with other authorities where people may file complaints. For example, if I file a complaint against Facebook — which has registered its main establishment in Ireland — in my home country of France, the Irish DPA will lead the investigation but will have to consult with the French authority as well as any other authority that may have an interest in the case to protect the rights of people living in their particular jurisdiction.

The system has yet to be fully tested but its complexity does not come as a surprise. In December 2015, during the negotiations of the GDPR, the legal services of the Council of the EU which represents the EU member states expressed concerns regarding the functioning of the one-stop-shop.[24] They indicated that "the lead authorities are a bad system if you want to protect citizens' fundamental rights", and noted further that while the system would be a one-stop-shop for companies, it would be "a three-stop-shop" for people, as we would have to deal with several authorities and courts to get a complaint resolved. So far, the system has indeed proven to be useful for companies which can benefit from having to deal with a single authority, but it is much more cumbersome for individuals and DPAs.

Why did lawmakers agree on such a complicated system? In an opinion on a case regarding the application of the one-stop-shop, Advocate General Bobek recalls the

[24] Kelly Fiveash, The Register, *EU legal eagle Legal: Data protection reforms 'very bad outcome' for citizens*, 2013. https://www.theregister.co.uk/2013/12/09/eu_data_protection_reforms_hits_legal_roadblock/

negotiations process of the system.[25] At the time, the Council and the Parliament made modifications to the Commission's original proposal so that all the power would not be in the hands of a single lead data protection authority in cross-border cases and to enhance the "proximity" between individuals and the supervisory authorities:

> *In essence, with the Council's and the Parliament's intervention, the one-stop-shop mechanism, previously heavily leaning towards the LSA [Lead Supervisory Authority], was turned into a more balanced two-pillar mechanism: the leading role of the LSA with regard to cross-border processing is preserved, but it is now accompanied by an enhanced role for the other supervisory authorities which actively participate in the process through the cooperation and consistency mechanisms, with the Board given the role of referee and guide in the event of disagreement.*[26]

It is important to recall that the one-stop-shop does not necessarily apply in all cross-border cases. In fact, the mechanism only applies when a company has declared a main establishment, which in turn leads to the designation of a lead authority. If no main establishment in the EU can be identified by the company or the regulators, then all data protection authorities would be competent to investigate cases. Finally, while it is up to companies to declare a main establishment, they still have to ensure that certain criteria are respected. In particular, the main establishment should be where "real" and "effective" management decisions related to data processing are taking place.[27] In some cases, such as with Google, companies have declared a main establishment for some, but not all, of their data activities. This means that in cases of complaints against Google, authorities will have to determine whether or not the data usage being challenged falls under the remit of the Irish authority which is linked to the main establishment in Ireland.

[25] Court of Justice of the European Union, Opinion of Advocate General Bobek, *C-645/19, Facebook v. Belgian Data Protection Authority*, 2020.
https://curia.europa.eu/juris/document/document.jsf?text=&docid=236410&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=6231046
[26] Ibidem.
[27] 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) (Text with EEA relevance), Recital 36.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

HOW IT IS GOING

While positive in principle, the cooperation mechanism designed under the one-stop-shop is difficult to apply in practice.

In our 2020 report, we indicated that out of all EU data protection authorities, only five report that they have enough resources to dedicate time to coordination tasks, including cross-border complaints.[28]

In fact, data protection authorities have been increasingly vocal on the numerous issues they face when seeking to apply the one-stop-shop. Several DPAs are talking of a "bottleneck" in the handling of cross-border cases, as lead authorities are neither being transparent nor moving quickly enough to process complaints. In 2020, Ulrich Kelber, the head of Germany's Federal DPA, called the functioning of the current cross-border enforcement system "unbearable".[29] The Hamburg DPA called the one-stop-shop mechanism "cumbersome, time consuming, and ineffective".[30]

From DPA's responses to a 2020 questionnaire on the implementation of the GDPR, we identified four main issues with the one-stop-shop:[31]

1. Communications between DPAs

Fourteen DPAs identified major issues related to communications and communication tools. All of them indicate that the system currently used at the EDPB level to follow cases — the Internal Market Information System (IMI) — is inadequate for their work.[32] Indeed, this system was not specifically created for the work of DPAs but is an existing EU system used for market monitoring in other areas of law. While we understand the practical aspect of not having to build a new tool, it appears that an overwhelming majority of DPAs considers this system not fit for purpose and that the lack of a tailored tool leads to communications being missed, deadlines being ignored, and other problems.

DPAs also noted a lack of clarity as to the type and volume of information that should be shared through the IMI to facilitate cooperation between the lead authority and

[28] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en
[29] Vincent Manancourt, POLITICO Europe, *EU privacy regulators voice alarm over GDPR, documents show,* 2020. https://pro.politico.eu/news/eu-privacy-regulators-alarm-problems-documents
[30] The Hamburg Commissioner for Data Protection and Freedom of Information, *Data Protection as fundamental right –big demand, long delivery time*, 2020. https://datenschutz-hamburg.de/assets/pdf/2020-02-13_press-release_annual_report_2019.pdf
[31] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en
[32] Ibidem.

concerned authorities. The lack of harmonisation in processes may lead to delays in cases.

2. Differences in national procedures

Nearly half of the DPAs indicated that the differences in national procedures related to the handling of complaints created issues with the application of the one-stop-shop.[33]

For instance, most EU states have different rules on individuals' right to be heard in a case, how to involve them in a case, and what information can be communicated back to them. These difficulties are not specifically due to the rules under the GDPR but show the need to harmonise procedures between states to ensure equal access to transparent and independent remedy across the EU.

Several DPAs, including the Spanish AEPD, note that these differences in procedures may result in a lead authority rejecting a complaint even if the local authority where the case was lodged had formally accepted it. The Swedish DPA notes that the differences in national procedures have an impact "on the possibility to cooperate effectively in cross-border cases" and in some cases this can lead to "forum shopping by the companies. This was not the intention of the OSS and the DPAs and the Commission must be vigilant to see any tendencies of such and make sure it is prevented".

3. Deadlines and lengthiness of processes

DPAs, including authorities from Germany, Luxembourg, and Ireland expressed frustration with the duration of processes under the one-stop-shop.[34]

Germany pointed out there are delays in cross-border cases when one authority has to serve as a lead authority in many cases. The German DPA added that the concept of a lead authority "may have advantages for companies, but it is complex for DPAs in practice. However, timely proceedings in cross border cases are essential for the effective enforcement of the GDPR and its acceptance". On the other hand, Ireland indicated that concerned authorities are sometimes slowing down the work of the lead authority, for instance "where it could take several months for a CSA to transmit complaint files to the

[33] Ibidem.
[34] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en and; Nicholas Vinocur, POLITICO Europe, *'We have a huge problem': European regulator despairs over lack of enforcement, 2019.* https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/

DPC as LSA. This led to months-long delays for data subjects in the handling of their complaints".[35]

Belgium noted that the lengthiness of resolution for cross-border cases compared to national cases poses competition risks, "whereas it is much easier to resolve national cases, sometimes leading to sanctions imposed on companies operating within the country, whereas similar infringements by multinational companies remain unsanctioned".[36]

In addition, the different steps under the one-stop-shop mechanism sometimes lack clear deadlines, in particular in cases of disagreement between the lead authority and the concerned authorities. It would help speed up the resolution of cases if EDPB developed clear deadlines to determine when lead authorities must provide revised decisions under Article 65 processes, for example.

4. Who is in charge?

The million ~~dollar~~ euro question: When is a lead authority *really* a lead authority? And can other authorities still act?

Several DPAs including authorities from Germany and Ireland are pointing to difficulties in identifying which DPA is the lead authority.[37] This point is particularly important as it determines who may be in charge of handling a complaint. Clarifying this point could help resolve some of the bottleneck issues DPAs are highlighting, where a small number of authorities are tasked with most cross-border cases.

A key aspect to resolving this problem centres around the identification of a main establishment. A company can declare an EU country to be its main establishment which in turn leads to the determination of its lead authority. However, certain criteria must apply for an entity to qualify as a main establishment: it must be the place where real and effective management decisions are taken regarding the processing of data.

---

[35] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en
[36] Ibidem.
[37] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en and;
Joseph Duball, IAPP, *EU grappling with potential one-stop-shop reform,* 2021. https://iapp.org/news/a/eu-grappling-with-potential-one-stop-shop-reform/

In practice, it is unclear how DPA assesses these criteria and companies may have been abusing this situation to pick main establishments in countries where they do not in fact conduct management of data processing. An investigative article published by *POLITICO Europe* provides information on the management structure within Amazon and the fact that the US-based entity maintains control over decisions regarding the handling of data, thus casting doubt as to whether Amazon Luxembourg can be considered a "main establishment" for the company.[38] Access Now wrote to the EDPB in April 2021 to seek clarification on the criteria used to determine a main establishment to help address these issues and ensure that corporations do not abuse the one-stop-shop.[39]

The Belgian DPA is also seeking clarification on how it can exercise its powers both within the one-stop-shop and in front of a national court, in a case that is now being heard by the Court of Justice of the European Union.[40] Advocate General Bobek's opinion in this case raises a number of issues relevant for the future if we see a lack of cooperation between DPAs and under-enforcement of the law.[41] Bobek puts forward suggestions as to when urgency procedures and other mechanisms provided for under the GDPR may be used to help improve the resolution of cases. Bobek defends the mechanism developed under the GDPR and notes that it would be too soon to pass judgment on its functioning, but also highlights the complexity of the system:

> *Having said that, it must be acknowledged that the two mechanisms illustrated above (Articles 61 and 66 of the GDPR on the one hand, and Articles 64 and 65 of the GDPR on the other hand), are somewhat cumbersome. Their actual functioning is not always crystal clear. Therefore, if on paper the above mentioned provisions seem apt to avoid those problems, only the future application of those provisions will tell whether, in practice, those provisions may turn out to be "paper tigers".*[42]

---

[38] Vincent Manancourt, POLITICO Europe, *Millions of people's data is at risk' — Amazon insiders sound alarm over security*, 2021. https://www.politico.eu/article/data-at-risk-amazon-security-threat

[39] Access Now, *Access Now's letter to the EDPB on the identification of a main establishment under the GDPR*, 2020. https://www.accessnow.org/cms/assets/uploads/2021/04/Access-Now-Letter-to-the-EDPB-Main-establishment.pdf

[40] Court of Justice of the European Union, *C-645/19, Facebook v. Belgian Data Protection Authority*. https://curia.europa.eu/juris/fiche.jsf?id=C%3B645%3B19%3BRP%3B1%3BP%3B1%3BC2019%2F0645%2FP&oqp=&for=&mat=or&lgrec=fr&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-645%252F19&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=fr&avg=&cid=367013

[41] Court of Justice of the European Union, Opinion of Advocate General Bobek, *C-645/19, Facebook v. Belgian Data Protection Authority*, 2020. https://curia.europa.eu/juris/document/document.jsf?text=&docid=236410&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=6231046

[42] Paragraph 122. Court of Justice of the European Union, Opinion of Advocate General Bobek, *C-645/19, Facebook v. Belgian Data Protection Authority*, 2020. https://curia.europa.eu/juris/document/document.jsf?text=&docid=236410&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=6231046

The Court of Justice is expected to deliver its ruling on this case on 15 June 2021.[43] It could bring much needed guidance and clarification on DPAs' powers and how they can use them. Beyond this case, the issues DPAs identified are significant and should not be left unheard. The increased frustration over the enforcement of the GDPR has led to tension between DPAs and has translated into public fights.[44] This situation is problematic for the cooperation between DPAs and the EDPB must urgently address it to avoid further internal disagreements that would render cooperation impossible.

From the first three years of the application of the GDPR, we can draw significant lessons for strengthening enforcement of the law. So far, the GDPR has been a legislative success but an enforcement failure. As DPAs carry the responsibility for enforcing the GDPR, it is important to provide them with adequate resources to exercise their tasks and address the shortcomings they identify. In Section III, we make recommendations to address the four areas for improvement we (and DPAs) have identified. We call on EU states and the DPAs not only to make the necessary structural and practical improvements, but also to put political will behind the enforcement of the GDPR.

As it stands, people's data protection rights are not being vindicated and the EU's flagship data protection legislation risks failing to deliver on its promise to do so. Unless the enforcement scales up, we risk returning to the "business as usual" scenario that existed under the 1995 Directive, when most companies ignored the law because the "risk" of enforcement and the fines were relatively low. This would undermine healthy competition in the EU single market. With enforcement lagging behind, companies that are not respecting the GDPR and are profiting from their privacy-invasive practices would have an unfair advantage over companies that play by the rules.

[43] Vincent Manancourt, POLITICO Europe, *EU court will rule on Facebook data protection case on June 15,* 2021. https://pro.politico.eu/news/eu-court-will-rule-on-facebook-data-protection-case-on-june-15
[44] Financial Times, *Fight breaks out between Ireland and Germany over Big Tech regulation*, 2021. https://www.ft.com/content/37705bcf-c5b6-4ef0-adb8-35a8680dbaec

II. RECOMMENDATIONS: MOVING THE GDPR FORWARD

To address the issues and challenges detailed in this report, Access Now has prepared recommendations directed at the European Commission, national governments, data protection authorities (DPAs), and the European Data Protection Board (EDPB). We believe that the implementation of these concrete recommendations will help ensure that the promise of the GDPR to strengthen the right to data protection will be effectively delivered across the EU.

RECOMMENDATIONS TO THE EUROPEAN COMMISSION	
CREATE NEW COMMUNICATION AND COLLABORATIVE TOOL FOR THE DPAS	The European Commission should work with the EDPB and the national DPAs to build a new communication platform for communications and handling of cross-border cases to replace the IMI system.
DEVELOP ADDITIONAL GUIDELINES TO CLARIFY ONE-STOP-SHOP PROCEDURES	The European Commission should work with DPAs, the EDPB, and EU states to develop guidelines to streamline one-stop-shop processes: ➔ Identify differences in national procedures and endeavour to develop a common set of rules on handling cases, including rules on the right to be heard, providing for clear deadlines for each step of the process when the GDPR does not provide one, and ensuring transparency of information.
LAUNCH INFRINGEMENT PROCEDURES	The European Commission should launch infringement procedures against EU states: ➔ When they do not provide sufficient resources to DPAs; ➔ When they do not guarantee the DPA's independence in status and in practices; and ➔ When countries have not fully implemented the GDPR (such as in Slovenia).

RECOMMENDATIONS TO THE NATIONAL DATA PROTECTION AUTHORITIES AND THE EUROPEAN DATA PROTECTION BOARD	
DEVELOP ADDITIONAL GUIDELINES TO CLARIFY TIMELINES WITHIN ONE-STOP-SHOP PROCEDURES	DPAs should work within the EDPB to develop internal guidelines to streamline one-stop-shop processes: ➔ Clarify or establish deadlines for every step within the processes from Articles 60 and 65 to increase the speed of resolution of cross-border cases. ➔ Provide clear deadlines for each step of these processes with the aim of resolving cases within a maximum of nine months.
INCREASE COOPERATION	DPAs should increase cooperation between each other to ensure the functioning of the one-stop-shop mechanism, including sharing information on cross-border cases within agreed timeframes and providing support to each other during investigations.
USE THE URGENCY PROCEDURE	DPAs should utilise the urgency procedure laid down in Article 66 of the GDPR to adopt temporary measures or to encourage other authorities to act rapidly to protect people's rights.

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

Three years into the application of the GDPR, everyone acknowledges the difficulties of enforcing this legislation. Data protection authorities, who are at the centre of the enforcement of the GDPR, are best placed to identify core issues with the operationalisation of the one-stop-shop and other enforcement mechanisms. DPAs have been speaking up, raising concrete issues they experience in their daily activities when seeking to enforce the GDPR. From communications struggles to difficulties in cooperating when there are different national legal procedures to the need for clarity on how to identify lead authorities, the issues raised by DPAs offer a path forward to significantly improve GDPR enforcement. The relevant parties can make these improvements without having to reform the GDPR itself, simply by clarifying certain procedures and providing DPAs with the appropriate tools and resources to do their jobs. We provide a set of recommendations to help facilitate the process, and we urge the European Commission, DPAs, and member states to work together to address these issues and unleash the power of the GDPR to improve people's lives.

A lot is at stake. Getting GDPR enforcement right is of paramount importance for effectively guaranteeing the right to data protection in the EU. It is also a vital step for ensuring fair competition in the EU single market, denying companies that do not comply with the GDPR an unfair competitive advantage over those that respect our rights and invest in protecting our data. Finally, improving enforcement is important for the EU's image. The success or failure of the GDPR will have implications beyond Europe, as many countries are drawing inspiration from this flagship regulation model. The European Union should also carefully consider lessons from the application of the GDPR and the functioning of its enforcement mechanisms as it develops future legislative instruments, such as the proposed Digital Services Act, Data Governance Act, and Artificial Intelligence Regulation.

Three years into the application of the GDPR, we can — and must — do better.

For more information, visit our Data Protection page:

accessnow.org/issue/data-protection