# TWO YEARS UNDER THE EU GDPR

## AN IMPLEMENTATION PROGRESS REPORT

### STATE OF PLAY, ANALYSIS, AND RECOMMENDATIONS

accessnow

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.

accessnow.org

**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 Fanny Hidvégi, Donna Wentworth, and Juliana Castro, as well as our Mozilla Fellow Daniel Leufer.

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

It has been two years since the EU General Data Protection Regulation (GDPR) entered into application. We have witnessed the first positive impacts of the law but also the challenges authorities, courts, and people have faced in its enforcement. The past 12 months have proven particularly demanding for the protection of personal data and the application of the law as the European Union — and the world — has faced significant political and health crises.

In our first GDPR progress report, published in May 2019, we wrote: "for most, 2018 was the year of data protection awakening in Europe. Still, for the GDPR to reach its full potential, 2019 must be the year of enforcement."[1] As it turned out, however, the last year has been a time of crisis. From public health to political crises, human rights abuses to administrative backlog, a series of challenges have put the robustness of the GDPR to test.

In this report, we look at how the multiple crises of the last year have impacted the application of the GDPR. We will start by addressing some of the internal challenges, wherein the mechanisms established for enforcement of the GDPR have begun to show their limitations, with a particular focus on the lack of cooperation among data protection authorities (DPAs) and the lack of resources to do their work. We will then analyse how external crises, such as the United Kingdom's decision to leave the European Union and the COVID-19 outbreak, are further challenging the application of the law. We close this report by putting forward a list of recommendations to enable the European Commission, EU states, and DPAs to address the hurdles here identified with the application of the GDPR.

May 2020 not only marks the second anniversary of the GDPR, it is also the first official review of the law to be conducted by the EU institutions.[2] Access Now has contributed to the process by providing comments to the European Commission through our membership in the multistakeholder expert group on the implementation of the law.[3]

[1] Access Now, *One year under the EU GDPR*, 2019.
https://www.accessnow.org/cms/assets/uploads/2019/07/One-Year-Under-GDPR-report.pdf
[2] European Union. *Article 97 of 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)*, 2016.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[3] Access Now. *Access Now's response to questions shared on the multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 - Questions to inform the preparation of the evaluation report of May 2020 on the application of GDPR*, 2020.

The publication of this report, coinciding with the review process of the law, is an opportunity to highlight the successes of the GDPR. These include its robustness and ability to provide human rights safeguards during crises; its role in advancing and protecting our rights in the EU; its capacity as a reference point globally, establishing the EU as a world leader in the field of data protection; and more. But we must also reflect on the challenges, such as how the law has been misused in efforts to silence journalists and NGOs, and how the slow pace of enforcement, exacerbated by the lack of cooperation between DPAs, has threatened to undermine the GDPR's long-term capacity to change private-sector norms and practices with regard to data protection.

In our report, we further note a disconnect between the rate of enforcement and the perception of enforcement by the public. Data show that DPAs have opened investigations and imposed fines at an exponentially increasing rate since May 2018. However, in some cases it is yet not clear what the impact will be of these enforcement measures, and we continue to wait for the resolution of landmark cases with the potential to force broad changes in invasive data-harvesting behaviour.

Opponents of the GDPR are meanwhile using the review process as an opportunity to seek a change of the text, and with it, to remove many of the provisions that safeguard our rights. It would be ill-advised for the EU to reform or re-open the GDPR before it has been adequately implemented, applied, and enforced.

It took the EU institutions and member states five years to negotiate the GDPR under immense external pressure to compromise, so it is perhaps not surprising that its application is not perfect two years in. But we will need more than patience to see the promises of the GDPR delivered. Concrete, urgent action is needed. It is imperative that DPAs work faster and in a more coordinated manner. 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. Fear of legal costs and delay tactics have sharply limited the capacity of DPAs to move forward key cases against tech giants whose revenues are sometimes ten times higher than the DPAs' budgets. To counter this imbalance, member states and the EU must give DPAs ample resources and protect their independence.

As the GDPR has withstood two years of tests, crises, and challenges, we call on the EU institutions and the DPAs to move forward with the application and enforcement of the law.

---

https://www.accessnow.org/cms/assets/uploads/2020/02/Access-Now%E2%80%99s-written-contribution-to-the-multi-stakeholder-expert-group-to-support-the-application-of-Regulation-EU-2016679-January-2020.pdf

# TABLE OF CONTENTS

# INTRODUCTION

Two years ago, the EU General Data Protection Regulation became applicable. During its first year, the GDPR led to an increase in awareness of data protection rights among citizens, governments, and businesses. Although we had high hopes that its second year would be focused on enforcement, it turned out to be a year full of challenges for the GDPR. Over the last 12 months, the law has faced administrative and political crises and has had to adapt to a public health crisis.

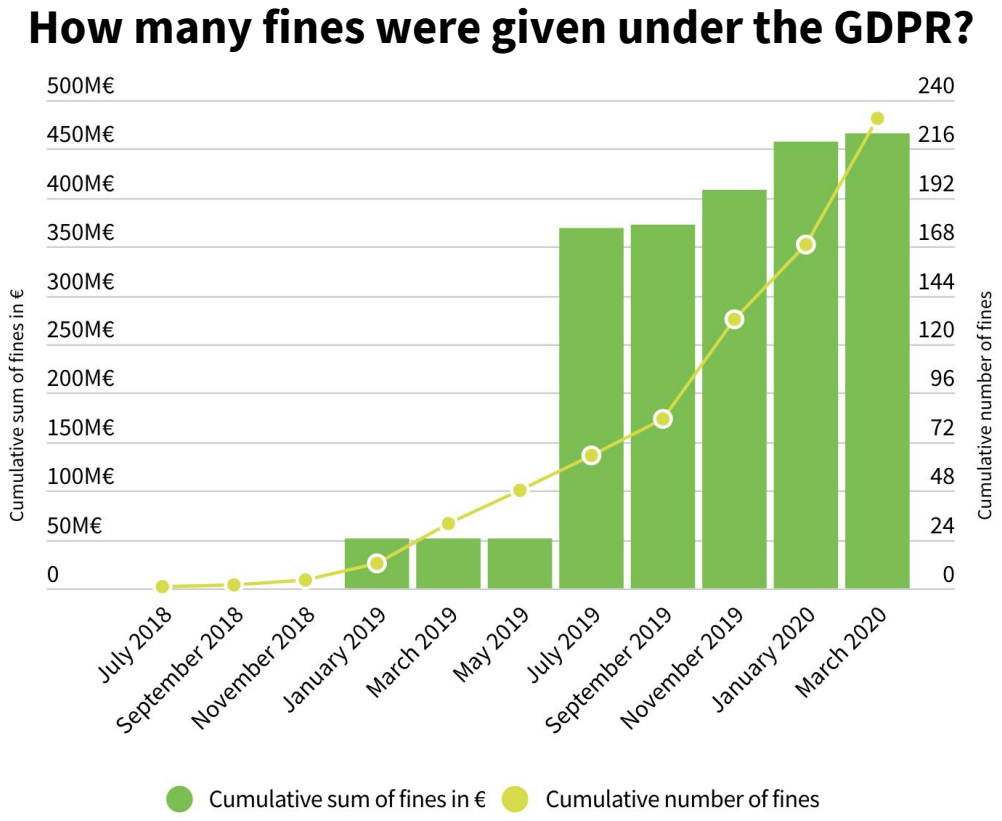
Data Protection Authorities (DPAs) struggled not only to work together but sometimes to work at all, straining their ability to enforce the law. The COVID-19 outbreak has tested the capacity of the law to provide for human rights protections in times of crisis. What is more, in a number of EU countries there have been attempts to misuse the GDPR to hurt the work of journalists and civil society actors. Finally, the United Kingdom's decision to leave the European Union has consequences for the application of the GDPR and implications for the protection of personal data in Europe.

In this report, we examine these challenges and provide recommendations to member states, the European Commission, and DPAs to address some of the most pressing shortcomings in the application of the GDPR.

# I. GDPR AND ENFORCEMENT: AN ADMINISTRATIVE CRISIS

## A. NOT FEELING (THE) FINES

In May 2019, Access Now published a report in which we highlighted several issues with the implementation and enforcement of the GDPR. At the time, we brought attention to the slow resolution of complaints.[4] Looking at the growth in the number and severity of sanctions and fines imposed since May 2018, it is clear Data Protection Authorities (DPAs) have significantly increased their GDPR enforcement activities.[5] However, the market and users have yet to feel the full impact of these enforcement actions.




Explore the interactive chart

From May 2018 to March 2020, DPAs levied **231 fines** and sanctions.[6] As shown in the graphic below, the number and size of these fines has grown exponentially since the

[4] Access Now, *One year under the EU GDPR*, 2019.
https://www.accessnow.org/cms/assets/uploads/2019/07/One-Year-Under-GDPR-report.pdf
[5] ZDNet, *Guess what? GDPR enforcement is on fire!*, 2020.
https://www.zdnet.com/article/guess-what-gdpr-enforcement-is-on-fire/
[6] This data as well as all figures from the first graphic and the list of fines are from: CMS, *GDPR enforcement tracker*, 2020.
https://www.enforcementtracker.com/?insights

GDPR became applicable. While this growth is positive, the total number of fines is still low compared to the **144,376 complaints** that people had filed by May 2019.

While not every complaint will result in a fine and other sanctions are available as a remedy for data protection violations, a large number of complaints remain unaddressed. DPAs are now facing a backlog of complaints. In addition to watching any investigations they may launch on their own, we are waiting for DPAs to respond to these complaints to protect our rights.

The **highest number of fines** came out of **Spain, with 81** so far, followed by Romania (26) and Germany (25). It shall however be noted that while most countries have only one DPA, due to the German federal system, the country has 17 separate DPAs, making the number of fines comparatively rather low.

When it comes to the size of fines, the **United Kingdom has imposed the largest total amount,** at more than **€315 million** to date. However, two of the biggest fines, imposed against British Airways (€204 million) and Marriott International (€110 million), have been **delayed** twice. They were scheduled to take effect, respectively, on May 18 and June 1. On May 12, however, the UK authority delayed Marriott's fine for the third time. A final decision on the fine is now expected to be taken on September 30, more than a year after the penalty was first announced.[7] Adding insult to injury, on the day the second delay was announced, Marriott confirmed their second data breach in three years, this time involving the personal information of 5.2 million guests.[8]

Following the UK is **France with just over €51 million in fines**. Nearly all of that total is due to the €51 million fine imposed on Google.[9] The company is currently appealing the decision.[10]

Ireland and Luxembourg, which are the main authorities dealing with the cases involving Amazon, Facebook, WhatsApp, Twitter, PayPal, Instagram, Microsoft, Google, and others, have issued **zero fines** against these tech giants to date. In the meantime, in 2018 and 2019, the Irish authority **received a total of 11,328 complaints**.[11]

[7] Politico EU, *UK again delays fine for Marriott's GDPR violations,* 2020.
https://pro.politico.eu/news/uk-again-delays-fine-for-marriotts-gdpr-violations
[8] TechCrunch, *Marriott says 5.2 million guest records were stolen in another data breach,* 2020.
https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?guccounter=1
[9] 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
[10] France 24, *Google to appeal 50-million-euro French data consent fine,* 2019.
https://www.france24.com/en/20190123-google-appeal-50-million-euro-french-data-consent-fine
[11] Data Protection Commission, *Data Protection Commission publishes 2019 Annual Report*, 2020.
https://www.dataprotection.ie/en/data-protection-commission-publishes-2019-annual-report

## Top 10 fines given under the GDPR

| COMPANY | AMOUNT IN € |
|---|---|
| British Airways | 204,600,000 € |
| Marriott International | 110,390,200 € |
| Google Inc | 50,000,000 € |
| TIM | 27,800,000 € |
| Austrian Post | 18,000,000 € |
| Deutsche Wohnen SE | 14,500,000 € |
| 1&1 Telecom GmbH | 9,550,000 € |
| Eni Gas e Luce | 8,500,000 € |
| Google LLC | 7,000,000 € |
| Eni Gas e Luce | 3,000,000 € |

Beyond fines, other important punitive sanctions have been imposed since May 2018. In the **UK**, the Data Protection Authority issued an **enforcement notice** against the government's tax office, after an investigation found that it had collected biometric data from millions of citizens without obtaining proper consent.[12] The notice ordered the tax office to **delete the database** containing all the information collected unlawfully. This landmark decision has an immediate effect on people's rights by not only addressing the initial data violation but also preventing further (mis)use of data. It also sends a strong signal to entities that failure to apply data protection rules creates more than financial liability.

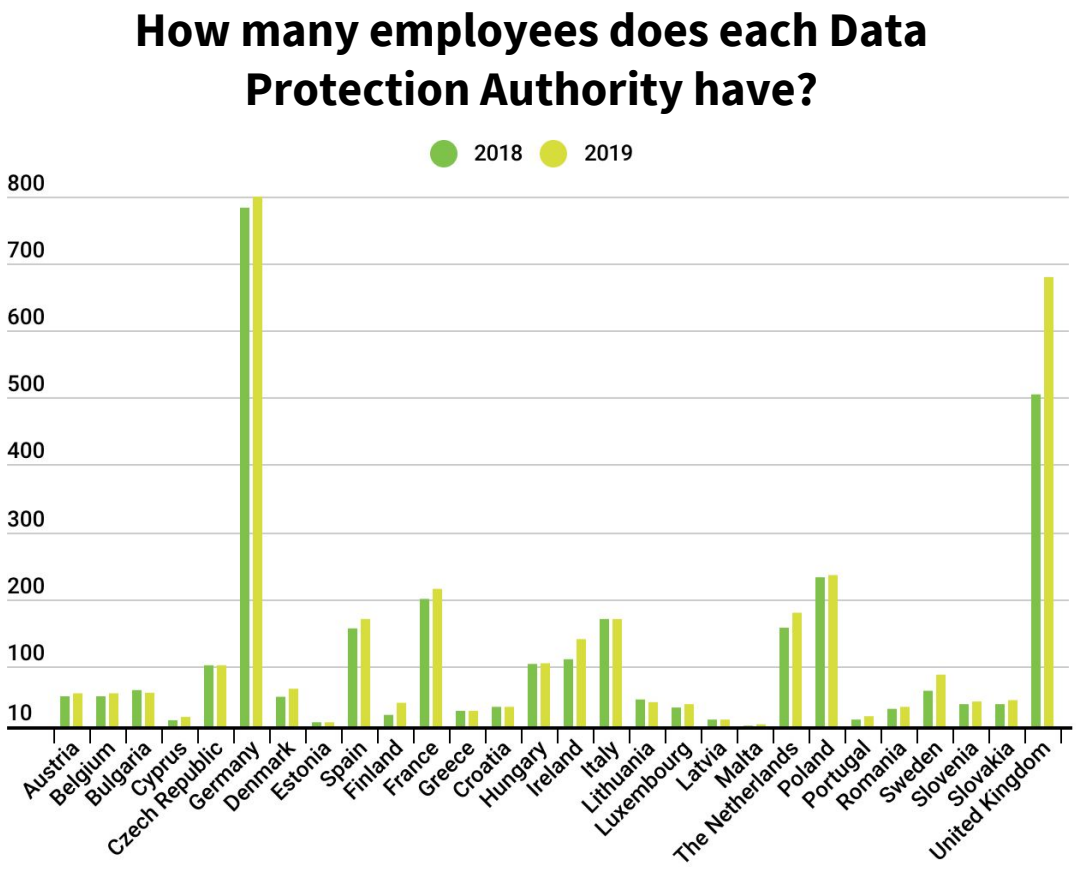
## B. DATA PROTECTION AUTHORITIES ARE LACKING RESOURCES

From the day of its adoption, we knew that awareness-raising, enforcement, and effecting a change in behaviour toward data protection would likely take time, as authorities need to provide guidance and re-organise their own functioning.

In last year's report we wrote: "Data Protection Authorities, as the main entities supervising and enforcing the GDPR, will play a central role in the success or failure of the law. To that end, it is of utmost importance that Member States respect and guarantee the independence of these authorities and to provide them with increased financial and human resources to ensure that they have the means to perform their tasks adequately".

[12] Information Commissioner's Office, *Enforcement Notice,* 2019.
https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf

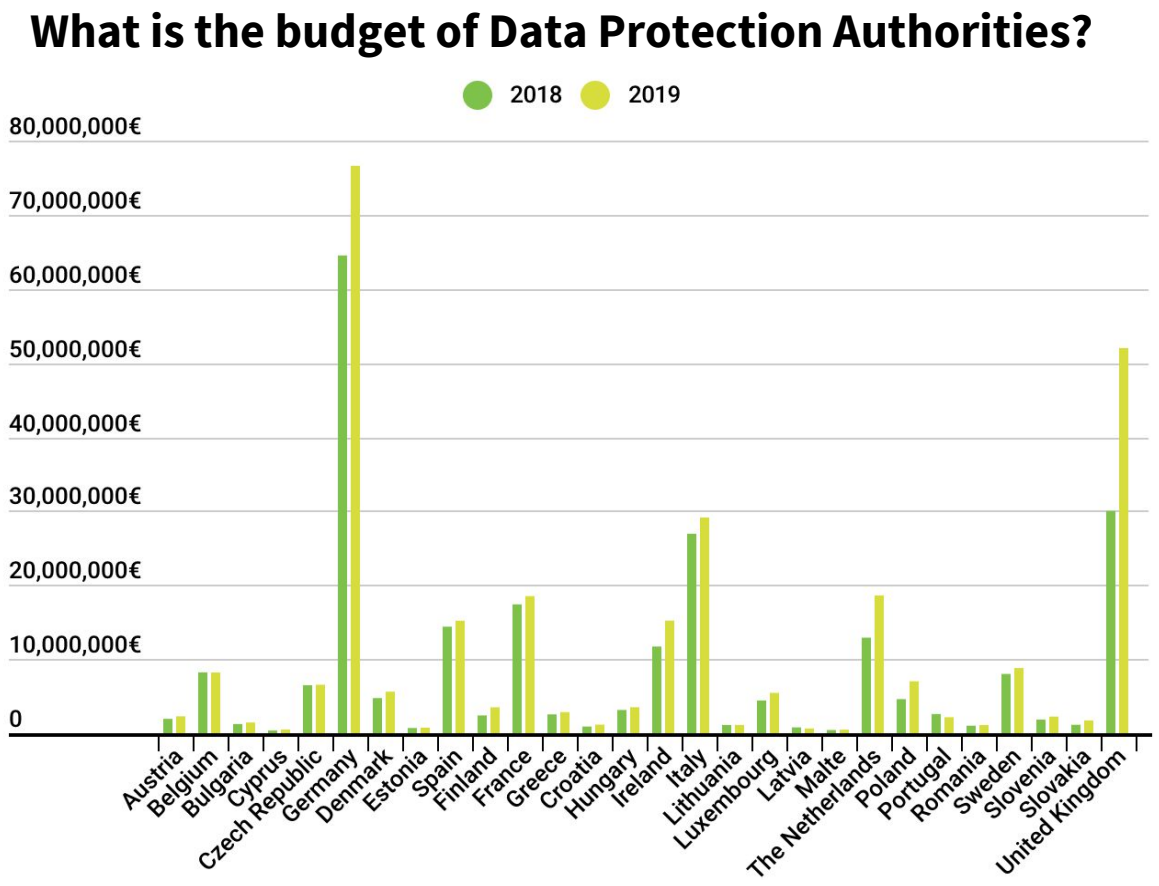
One year later, the situation has not improved. As shown in the graphic below, the number of employees working in Data Protection Authorities across the EU has barely increased from 2019. According to information shared by the authorities with the European Data Protection Board (EDPB), the number of staff across the EU will largely stay the same for 2020.[13]




Explore the interactive chart

At the center of the success or failure of the GDPR are the Data Protection Authorities. If they do not enforce the law, we as individuals may never experience its benefits. For DPAs to function properly and address the large number of complaints that have been filed, the resources allocated to them must be increased. *Politico Europe* reported that many DPAs have been expressing their dissatisfaction with their current budget and resources.[14] Out of 30 DPAs from all 27 EU countries, the United Kingdom, Norway, and Iceland, only nine said they were happy with their level of resourcing.[15]

[13] Data from the following two graphics are from: European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en
[14] Politico EU, *EU privacy regulators voice alarm over GDPR, documents show,* 2020. https://pro.politico.eu/news/eu-privacy-regulators-alarm-problems-documents
[15] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en




Explore the interactive chart

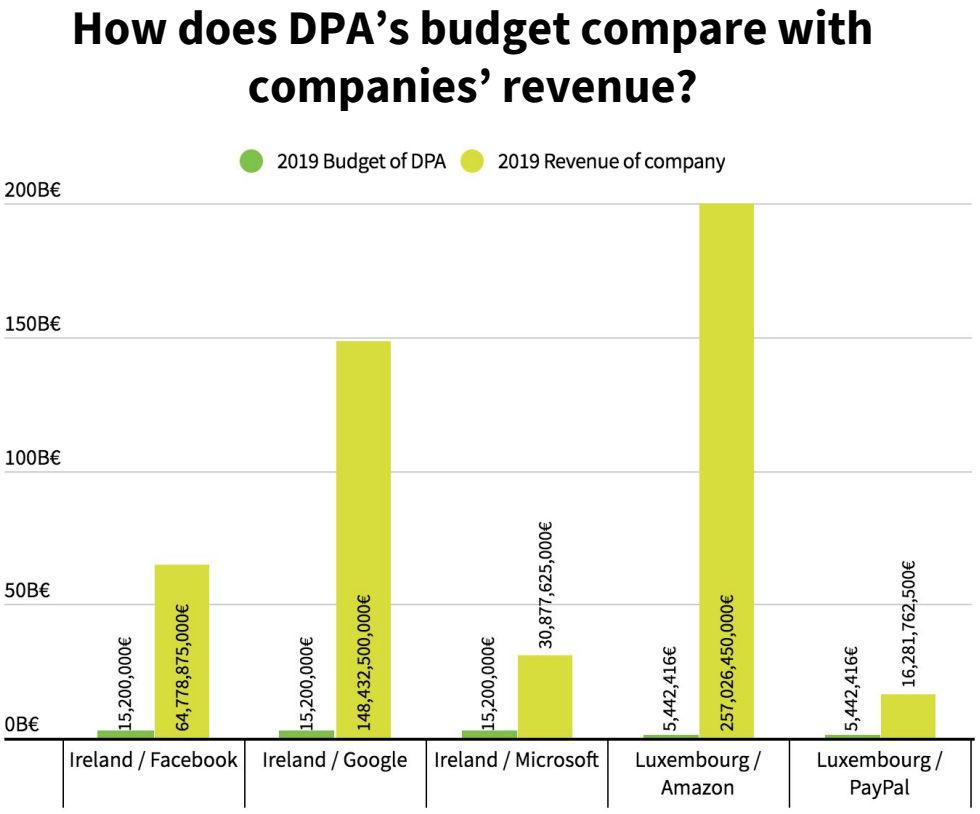
The graphic above shows significant disparities in budget between authorities across the EU. While Germany tops the charts in both staffing and funding, these resources are spread across the 17 authorities, one for each of the 16 local states and a federal one. The United Kingdom is therefore the authority with the most staff and financial resources. It is also one of the few authorities to have in-house technological expertise, which is extremely important in conducting independent investigations.[16] As the UK is set to exit the European Union, the network of European authorities working together within the EDPB will lose the support of this highly resourced authority.

The UK's budget is double that of Italy and three times bigger than that of France, even though the three countries have roughly the same number of inhabitants and their economies are similar in size. And no, this does not mean that the UK has too big a budget; it may actually be the only authority with adequate resources. EU states are failing and leaving their DPAs in a critical situation. If DPAs do not have adequate resources, we risk a return to the "business as usual" scenario that we experienced under the 95/46 Directive, when many companies ignored the law because enforcement was either slow or nonexistent.

[16] Brave, *Europe's governments are failing the GDPR*, 2020. https://brave.com/dpa-report-2020/

The inadequate budget provided to DPAs means that our rights may not be effectively protected. In fact, it may create a negative incentive for DPAs investigating large tech companies to agree on settlements that may be more favourable to the companies. The UK authority reached a settlement with Facebook following the Cambridge Analytica scandal and it is believed the authority opted for this avenue to limit the cost of lengthy proceedings.[17] This is particularly striking as the UK authority is one of best-resourced DPAs.

Companies could leverage DPAs' lack of resources, using it to get around the application of the GDPR, or at least significantly delay its effect. The Irish authority has for instance indicated that "procedural queries" from companies are delaying what would be their first fines.[18] In fact, Data Protection Authorities often lack the financial resources to enter into lengthy legal proceedings, which involve several layers of appeals, while companies are not so constrained.




Explore the interactive chart

[17] Information Commissioner's Office, *Statement on an agreement reached between Facebook and the ICO,* 2019. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/

[18] The Irish Times, *Big tech 'procedural queries' delay decision on first data fines – watchdog*, 2020. https://www.irishtimes.com/business/technology/big-tech-procedural-queries-delay-decision-on-first-data-fines-watchdog-1.4178751

The graphic above illustrates the disparity of resources between Data Protection Authorities and the companies they are supposed to keep in check. Large tech companies have nearly endless financial resources in comparison to the restrictive budget allocated to Data Protection Authorities. In the case of Ireland, the revenue of some of these companies is even higher than the Gross Domestic Product of the country.[19]

It is crucial that EU states allocate significantly more resources to DPAs. In a letter sent to the European Commission as part of the first review of the GDPR, the European Parliament has called for the start of infringement proceedings against national governments for failing to properly resource their DPAs.[20] While we hope that EU states will comply with their obligation to provide DPAs with adequate resources on their own, we support intervention from the European Commission to ensure that the application of the GDPR is not further delayed and jeopardised.

## C. ONE-STOP-SHOP: IS THE COOPERATION SYSTEM BROKEN?

Resources and budgets are major issues for the appropriate and timely application of the GDPR but there is another major administrative hurdle: the cooperation system within the European Data Protection Board. The GDPR establishes a complex mechanism for cooperation and consistency in the application of the law, which should, for example, serve in 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, we as users can bring a data protection complaint to the authority in the country where we live, even if the company against which we lodge the complaint is located in another country. Meanwhile, companies can designate a lead authority which will be tasked with handling all complaints about them, 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 is registered in Ireland — in my home country of France, the Irish Authority will lead the investigation but will have to consult with the French authority, which represents my rights, 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.

Two years after the GDPR became applicable, and despite the fact that many cross-border cases have been submitted to authorities, the system has yet to be fully tested for the resolution of cross-border cases. The complexity of the application of the system does not

[19] Politico EU, *How one country blocks the world on data privacy,* 2019.
https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123
[20] LIBE Committee, *Letter to Commissioner Reynders,* 2020.
https://www.politico.eu/wp-content/uploads/2020/03/SKM_C45820030616021.pdf

come as a surprise. In December 2015, during the negotiations of the GDPR, the legal services of the Council which represents the EU states expressed concerns regarding the functioning of the one-stop-shop.[21] 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. At the time, these concerns were regarded as highly political, as they risked the extension of already lengthy negotiations of the law. Two years into the application of the law, these comments do unfortunately summarise the current situation.

Several Data Protection Authorities are calling out the bottleneck of cross-border cases, as leading authorities are neither being transparent nor moving quickly enough to process complaints. Earlier this year, Ulrich Kelber, the head of Germany's federal Data Protection Authority, called the functioning of the current cross-border enforcement system "unbearable".[22] A few months later, the Hamburg DPA called the one-stop-shop mechanism "cumbersome, time consuming and ineffective".[23]

One of the major hurdles for cooperation is, once again, budget and resources. Out of all EU countries, only five considered that they have enough resources to dedicate time to coordination tasks, including cross-border complaints.[24] The five countries are the Czech Republic, Denmark, Hungary, the UK (which left the EU), and Luxembourg (which has yet to resolve any major case). All other countries report major issues. In the same survey, the Austrian Data Protection Authority said that they are not equipped to deal with some cases requiring cooperation with other authorities because "[a] lawyer of the authority is dealing with more than 100 cases (national and cross-border) simultaneously at an average". Many countries, including Belgium, Lithuania, Poland, and Bulgaria indicated that the authority does not have staff allocated to this cooperation. The 17 German authorities collectively indicated that "the current staffing is not found to be sufficient for the effective performance" of cooperation tasks. The Spanish authority notes that while they have more staff since 2018, "the increase in staff is insufficient to meet the growth in workload derived from the GDPR". The French authority indicates that it lacks the human resources to "effectively contribute to all cooperation mechanisms". Portugal's situation is the most alarming as "there is only one person (almost entirely) dedicated to that task".

[21] 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/
[22] Politico EU, *EU privacy regulators voice alarm over GDPR, documents show,* 2020. https://pro.politico.eu/news/eu-privacy-regulators-alarm-problems-documents
[23] 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
[24] European Data Protection Board, *Individual replies from the data protection supervisory authorities,* 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

With the one-stop-shop and the power granted to the lead authority, Ireland has a central role in the application of the GDPR. The Irish authority is responsible for handling a large number of cases, as many tech companies are registered in Ireland. The authority has yet to activate the cooperation mechanism within the EDPB but says that it "would welcome participation by EDPB colleagues in joint operations to collaborate" with its staff. The disproportionate weight put on a single authority for the application of the GDPR was precisely what the one-stop-shop was supposed to avoid. The fact that Ireland is currently leading a large number of GDPR complaints is not only an administrative issue but also potentially a political one. As a result of more than 70 years of economic transformation which encouraged foreign investment, in particular from the US, Ireland has become a safe haven for tech giants. In the 80's, tech companies such as Apple, Microsoft, Dell, and Intel established manufacturing plants in the country, taking advantage of significant tax cuts and establishing themselves as major investors and employers. As the years passed and as more companies established their European base in Ireland, tech giants have arguably gained an unprecedented level of influence in policy debates in Ireland. Reports have revealed how tech executives pressured the Irish government to protect their beneficial tax arrangements.[25] Now, data protection enforcement has also become a target for lobbying.[26] With pressure coming from both tech giants and the Irish government itself, the Irish Data Protection Commissioner's (DPC) ability to make full use of its powers, including imposing fines against these large companies for GDPR violations, remains questionable. The DPC has opened several investigations since the entry into application of the GDPR, but two years later, we are still waiting for the first major decision from Ireland.

As tech companies seek to avoid falling under the jurisdiction of other Data Protection Authorities, even if they process the data of users across the EU, we must prevent forum shopping in the protection of personal data. In that context, the European Commission and the European Data Protection Board have a central role in ensuring the proper functioning of the cooperation and consistency mechanisms. While we do not see a need to reform rules designed under the GDPR yet, we do stress the need to ensure that all the options provided by the law are utilised. We therefore urge DPAs to start utilising the urgency procedure laid down in Article 66 of the GDPR to adopt temporary measures or to force other authorities to act.[27]

[25] Politico EU, *How one country blocks the world on data privacy,* 2019.
https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123
[26] Politico EU, *How one country blocks the world on data privacy,* 2019.
https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123
[27] European Union. *Article 66 of 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)*, 2016.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

# II. THE GDPR IN TIMES OF POLITICAL, HEALTH, AND HUMAN RIGHTS CRISES

## A. GDPR & HEALTH CRISIS

Since its outbreak in late 2019, the world has been fighting the spread of COVID-19. In response to what the World Health Organisation (WHO) has labeled a pandemic, governments across the globe have been using data to map the spread of the virus and keep people safe. The rushed responses and acceptance of the often ill-conceived techno-solutionism evangelised by many companies underscore the need to protect fundamental rights, including the right to data protection, in all the measures aimed at addressing this public health crisis. While the European institutions and governments all reiterated the necessity of compliance with the GDPR, and DPAs highlighted how the law provides for flexibility, many responses have fallen short of EU standards for privacy and data protection.

Health information is private and sensitive by nature and reveals intimate details of a person's life. The use, collection, and any other processing of this information should be protected, ideally through a comprehensive data protection law like the GDPR.[28] Use of health information — ranging from blood type, medical pre-conditions, genetic information, temperature records, and more — is usually strictly limited. Nevertheless, during a public health crisis, the question is not *if* governments can use health data to help fight the crisis but *how* this can be done while safeguarding individual privacy and dignity to the maximum extent possible.

The NGO noyb indicated that "[c]ontrary to many initial reports, there is no general conflict between data protection, especially the GDPR, and the use of personal data in the fight against an epidemic. Statements claiming that data protection must [be] 'waived' seem to be based on a false understanding of law".[29]

In fact, the GDPR explicitly provides rules for data processing in the context of a public health crisis, in particular in Articles 6, 9, and 25, on, respectively, the legal basis for processing data, the specific measures applicable to the processing of sensitive data, and the requirement for data protection by design and by default. In particular, recital 46 specifically explains that "Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when

[28] Access Now, *Creating a data protection framework: A do's and don'ts guide for lawmakers,* 2018. https://www.accessnow.org/data-protection-handbook
[29] Noyb, *Data protection in times of coronavirus: not a question of if, but of how,* 2020. https://noyb.eu/en/data-protection-times-corona

processing is necessary for humanitarian purposes, including for *monitoring epidemics* [emphasis added] and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters".[30] The GDPR can and must therefore be observed throughout the crisis and can help ensure that public health officials get access to the accurate and necessary data to fight the outbreak.

In an aggressive yet unsurprising move, the Hungarian government decided in May 2020 to suspend the application of a number of core data protection rights protected under Articles 15 to 22 of the General Data Protection Regulation as part of "the coronavirus emergency measures". Rights affected include the right to access your data, the right to be informed about how your data are being used, the right to object to the processing of your data, and more.[31] The government further established time limits for the exercise of remedy rights, including the right to lodge a complaint and the right to an effective judicial remedy, guaranteed by Articles 77-79 of the GDPR. This decision is disproportionate and gravely endangers people's right to data protection at a time when our personal information, including our health data, is being collected perhaps more than ever. Together with the Hungarian Civil Liberties Union and Civil Liberties Union for Europe, Access Now wrote to the European Data Protection Board, calling on them to ask the European Commission to launch an infringement procedure against Hungary to restore the application of data protection rights.[32]

In combating COVID-19, public authorities should be able to rely on data, including health data, to determine the best course of action to mitigate the spread of the virus and identify what measures must be taken to safeguard people and their rights during and after the crisis.[33]

The COVID-19 pandemic continues to spread as we write this report, and it will be crucial to ensure that this public health crisis does not turn into a human rights crisis. Some EU states are implementing tracking programs and developing invasive contact-tracing apps. In the broader context of adopting emergency legislation and derogating from human rights obligations, national DPAs and the EDPB will have a crucial role in

[30] European Union. *Articles 6, 9, and 25 and recital 46 of 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)*, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[31] Magyar Közlöny, *A Kormány 179/2020. (V. 4.) Korm. rendelete a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről*, 2020. https://magyarkozlony.hu/hivatalos-lapok/8kGGfNvTeu9K9vNlCUoB5eab3bea8b653/dokumentumok/008772a9660e8ff51e7dd1f3d39ec056853ab26c/letoltes

[32] Access Now, Hungarian Civil Liberties Union and Civil Liberties Union for Europe, *NGO Joint letter to the EDPB on Hungary's decree limiting the application of the GDPR,* 2020. https://www.accessnow.org/cms/assets/uploads/2020/05/Joint-letter-to-EDPB-Hungary-GDPR-Decree-Access-Now-Liberties-HCLU.pdf

[33] Access Now, *Recommendations on privacy and data protection in the fight against COVID-19,* 2020. https://www.accessnow.org/releases-recommendations-on-privacy-data-protection-covid-19/

maintaining scrutiny over measures impacting data protection. The GDPR is a robust tool to guide officials and public health authorities in this crisis.

## B. GDPR & HUMAN RIGHTS ABUSES

In its two years of existence, the GDPR has proven to be a go-to tool for the exercise of our data protection rights. Unfortunately, a number of public authorities have tried to misuse the law to stifle journalism and undermine the work of civil society.

In Hungary, a court adopted a preliminary injunction obliging the local publisher of *Forbes* to recall from newsstands the issue of the magazine featuring a list of the richest Hungarians.[34] The court's decision was prompted by a complaint from Hell Energy Drink, a large domestically owned energy drink manufacturer. The company's leadership were evidently annoyed by the appearance of its owners on the list. Hell Energy Drink argued that *Forbes* breached its owners' right to data protection. Although the decision was not final, the magazine was immediately withdrawn from newsstands and the names of Hell Energy Drink's owners were removed from the online version of the list.

While several provisions of the GDPR, in particular Article 85, make explicit reference to the connection between the right to data protection and the right to freedom of expression, the court failed to adequately take free expression into account. It ought to have dismissed the complaint on free expression grounds. By doing the opposite, it gave legitimacy to an invalid complaint, undermined the newspaper's right to freely impart information, and jeopardised the application of the GDPR, as the law was then portrayed as "a road to hell".[35]

In Poland, an NGO faced a complaint for violating the GDPR through providing access to public information via a search engine for data from public registers, including data from the Polish National Court Register.[36] The Polish Data Protection Authority ordered the NGO to remove personal data included in the database as it considered this information to be sensitive data.[37] However, the NGO did not originally publish this information, which was obtained from a publicly available government source. The NGO ultimately won the case, as access to public information must be balanced with the right to data protection.[38] The NGO had to spend its limited resources to argue the need for this

[34] Forbes, *Bírósággal tüntetik el az utcákról a Forbes magazin gazdaglistáját a Hell Energy tulajdonosai,* 2020. forbes.hu/uzlet/birosaggal-tuntetik-el-az-utcakrol-a-forbes-magazin-gazdaglistajat-a-hell-energy-tulajdonosai/
[35] Center for Media, Data and Society, *GDPR in Hungary: A Road to Hell?*, 2020. https://medium.com/center-for-media-data-and-society/gdpr-in-hungary-a-road-to-hell-3b60718a0281
[36] Global Data Review, *Mixed messages from Poland: the uneasy relationship between regulations on reuse and the GDPR,* 2019. https://globaldatareview.com/mixed-messages-poland-uneasy-relationship-between-regulations-reuse-and-gdpr
[37] Wyborcza.pl*, Chciał ukryć swoje związki z organizacjami nacjonalistów. Sąd: Bycie narodowcem to nie tajemnica*, 2019 https://wyborcza.pl/7,75398,25340293,chcial-ukryc-swoje-zwiazki-z-organizacjami-nacjonalistow-sad.html
[38] Supreme Administrative Court, *II SA/Wa 562/19 - Wyrok WSA w Warszawie*, 2019. http://orzeczenia.nsa.gov.pl/doc/789C1A4811

balancing, even though that is explicitly acknowledged in the GDPR. Worse, the initial decision by the Polish Data Protection Authority has put into question its independence and the ability of the regulator to appropriately conduct this careful balancing of rights.

In Romania, one of the first cases under the GDPR unfortunately involved a scandal where the DPA itself tried to abuse the law to curtail investigative journalism. In November 2018, the Romanian Data Protection Authority sent a series of questions to the journalists who published information about the scandal, asking for their sources and mentioning the possibility of a data protection infringement penalty that would have been the biggest since the GDPR entered into force in May 2018: up to 20,000,000 euro.[39] The Data Protection Authority in Slovakia has employed similar tactics, threatening to fine journalists if they refused to reveal their sources. These misguided actions by DPAs are an attack on press freedom and a gross misuse of the GDPR.[40] In such cases, the authorities tasked with protecting our rights are doing exactly the opposite, thereby undermining the purpose of the GDPR.

In Slovakia, there is an even more alarming tale of GDPR misuse. In April 2020, the Slovak Parliament adopted a decision to remove Soňa Pőtheová, the head of the Data Protection Authority, from office for abusing her powers by seeking to force journalists to reveal their anonymous sources under the threat of disproportionate fines.[41] Further, an investigation of the 2018 murder of a journalist, Jan Kuciak, and his fiancé, Martina Kusnirova, revealed that Pőtheová had a direct connection to Marian Kocner, the Slovak businessman accused of ordering the murder.[42] Kuciak was an investigative journalist who delved into cases of fraud involving businessmen with political connections. The murder of Kuciak and his fiancé led to anti-corruption protests, and this has brought down the government of long-time Slovak Prime Minister Robert Fico.

The GDPR is a landmark law that contributes to the protection and guarantee of rights; not only the right to data protection but also the rights to freedom of expression, access to information, and other rights. The European Commission cannot allow national authorities, and in particular Data Protection Authorities, to misuse and misinterpret the GDPR in a way that would restrict freedom of the press or stifle NGOs' work. If actions are

[39] GDPRToday, *European Commission urged to investigate Romanian GDPR implementation,* 2019. https://www.gdprtoday.org/european-commission-urged-to-investigate-romanian-gdpr-implementation/
[40] European Parliament, Parliamentary Questions, *Subject: Abuse of power by Slovak data protection authority and threat to investigative journalism,* 2020. https://www.europarl.europa.eu/doceo/document/E-9-2020-001520_EN.html
[41] Dennikn, *Parlament odvolal Soňu Pötheovú, ktorej úrad pre Kočnera šikanoval novinárov,* 2020. https://dennikn.sk/minuta/1876221/?ref=list and; Pravda, *Parlament odvolal predsedníčku Úradu na ochranu osobných údajov Pötheovú*, 2020.https://spravy.pravda.sk/domace/clanok/550110-parlament-odvolal-predsednicku-uradu-na-ochranu-osobnych-udajov-potheovu/
[42] Euractiv, *Contract killer tells court how he murdered Slovak journalist and his fiancee*, 2020. https://www.euractiv.com/section/elections/news/contract-killer-tells-court-how-he-murdered-slovak-journalist-and-his-fiancee/

not taken to address and eliminate such behaviour, the GDPR could ultimately be perceived as a tool for oppression despite the fact that its aim is precisely the opposite.

## C. GDPR & BREXIT

The United Kingdom's decision to leave the European Union ("Brexit") will have significant consequences for both parties involved, including in the area of data protection.

First, in practical terms, since the departure of the UK on January 31, 2020, the UK Data Protection Authority is no longer a member of the European Data Protection Board. This means that the EU is losing its most well-resourced DPA, which provided much-needed technical expertise for complex investigations and a large number of staff that could contribute to cross-border cases.

While the UK had initially committed to continuing to observe the measures provided for under the GDPR even after its departure, Prime Minister Boris Johnson has made claims which suggest the opposite.[43] The UK is now reportedly insisting on lowering current standards through the Brexit talks and asking to deviate from agreed mechanisms of data protection.[44] We could see the UK developing its own data protection regime in the years to come, although, as with every aspect of Brexit, nothing is certain at this point. This will of course have implications for businesses operating both in the EU and the UK which would then have to comply with two different sets of rules. It also has implications for any future negotiations of a so-called adequacy decision between the EU and the UK that would authorise the transfer of data between the two jurisdictions.

The EU and the United Kingdom have clearly expressed their willingness to finalise an adequacy decision by the end of the transition period set by the withdrawal agreement.[45] As this period is currently set to conclude on December 31, 2020, these would potentially be the fastest-ever negotiations for an adequacy decision. We note that there is no obligation for the EU to finalise negotiations by then and that this date is merely a wish expressed by the parties. Negotiating an adequacy decision is not straightforward and this is not a done deal. In the past, negotiations with other countries have taken several years and the more divergent a system is, the longer it takes to analyse. Through the

[43] Euractiv, *UK to diverge from EU data protection rules, Johnson confirms,* 2020.
https://www.euractiv.com/section/digital/news/uk-to-diverge-from-eu-data-protection-rules-johnson-confirms/
[44] European Union, *Remarks by Michel Barnier following Round 3 of negotiations for a new partnership between the European Union and the United Kingdom*, 2020.
https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_895
[45] European Commission, *Slides - Internal EU27 preparatory discussions on the future relationship: "Personal data protection (adequacy decisions); Cooperation and equivalence in financial services",* 2020.
https://ec.europa.eu/commission/publications/slides-internal-eu27-preparatory-discussions-future-relationship-personal-data-protection-adequacy-decisions-cooperation-and-equivalence-financial-services_en

negotiations, the EU is supposed to determine whether the UK has an "essentially equivalent" level of data protection. Again, if the UK decides not to adhere to the rules under the GDPR any longer, the analysis of norms may take more time.

While the UK currently has the obligation to apply the GDPR, it will be crucial to ensure that the country continues to apply high standards for data protection going forward. In addition, as established by EU jurisprudence, the UK will have to guarantee EU data subjects' right to remedy and it will have to ensure that the processing of data by public authorities, including law enforcement authorities, is necessary and proportionate. One of the main components of any adequacy decision is the review of measures that could impinge on data and privacy rights, including surveillance measures. The UK has one of the most invasive surveillance systems in Europe, and may not reach an adequacy decision unless it undertakes massive reform.[46] The Commission has the obligation to ensure that data of people living in the EU will not be misused or intercepted for surveillance once it reaches the UK.

While negotiations on Brexit have been delayed due to the COVID-19 pandemic, recent revelations of data violations by the UK government mean that these talks are already setting off on the wrong foot. Over the past few months, we have learned that the UK Department of Health and Social Care has been selling patient data to drug companies.[47] Later on, it was revealed that the UK authorities illegally copied the EU Schengen Information System, a vast database used by police and border guards across the EU's border-free Schengen zone.[48] The UK was also found to be hiding information from its EU counterparts regarding cross-border investigations. [49]

While the UK may be leaving the European Union, it is not leaving Europe and ties between the country and the continent will remain, even if not without challenges.[50] For the benefit of UK citizens and everyone living in the UK, we call on the government to continue to apply the GDPR and to reform its surveillance laws.

[46] Wired, *The UK's mass surveillance regime has broken the law (again)*, 2018.
https://www.wired.co.uk/article/uk-mass-surveillance-echr-ruling
[47] The Guardian, *Revealed: how drugs giants can access your health records,* 2020.
https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data
[48] The Guardian, *UK accused of 'behaving like cowboys' over EU database copying,* 2020.
https://www.theguardian.com/world/2020/jan/09/uk-accused-of-behaving-like-cowboys-over-eu-database-copying
[49] The Guardian, *Revealed: UK concealed failure to alert EU over 75,000 criminal convictions,* 2020.
https://www.theguardian.com/uk-news/2020/jan/14/revealed-uk-concealed-failure-to-alert-eu-over-75000-criminal-convictions
[50] The Independent, *Boris Johnson refuses to commit to keeping UK in human rights convention,* 2020.
https://www.independent.co.uk/news/uk/politics/boris-johnson-brexit-human-rights-convention-echr-michel-barnier-a9378141.html

# III. 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, governments, Data Protection Authorities, and the European Data Protection Board. 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.

| 1. RECOMMENDATIONS TO GOVERNMENTS | |
|---|---|
| **INCREASE RESOURCES FOR DPAs** | To function properly and be able to address the large number of complaints, governments across the EU must increase the financial and human resources allocated to Data Protection Authorities, including technical staff. |
| **GUARANTEE DPAs' INDEPENDENCE** | Governments must guarantee the independence of Data Protection Authorities, both in statutes and financially. |
| **GOVERNMENTS MUST UPHOLD HUMAN RIGHTS DURING CRISES** | International and national laws recognise that extraordinary crises require the use of extraordinary measures. This means that certain fundamental rights, including the rights to privacy and data protection, may be restricted to address crises as long as basic democratic principles and a series of safeguards are applied, and the interference is lawful, limited in time, and not arbitrary. |
| **GOVERNMENTS MUST UPHOLD THE GDPR DURING THE COVID-19 CRISIS** | Governments should ensure the application of the GDPR and the protect the right to data protection in their COVID-19 response, particularly in the areas concerning the collection and use of health data, the use of tracking and geolocation, and the conclusion of public-private partnerships for the development and deployment of contact-tracing apps. |
| **THE UK MUST UPHOLD HUMAN RIGHTS BEYOND BREXIT** | For the benefit of UK citizens and everyone living in the UK, the UK government must continue to apply the GDPR and reform its surveillance laws. |

## 2. RECOMMENDATIONS TO THE EUROPEAN COMMISSION

| | |
|---|---|
| **LAUNCH INFRINGEMENT PROCEDURES** | The European Commission should launch infringement procedures against EU states :<br>➔ When they do not provide sufficient resources to Data Protection Authorities, or<br>➔ When they do not guarantee the Data Protection Authority independence in status and in practices, or<br>➔ Where Data Protection Authorities or courts misuse the GDPR to restrict freedom of the press or stifle NGOs' work. |
| **REVIEW ADEQUACY DECISIONS AND CONDUCT THOROUGH REVIEW OF UK DATA PRACTICES** | The European Commission shall review all existing adequacy decisions concluded prior to May 2018.<br>In its negotiations for an adequacy decision with the UK, the European Commission has the obligation to ensure that data from EU data subjects will not be misused or intercepted for surveillance once it reaches the UK. |

## 3. RECOMMENDATIONS TO THE NATIONAL DATA PROTECTION AUTHORITIES AND THE EUROPEAN DATA PROTECTION BOARD

| | |
|---|---|
| **INCREASE COOPERATION** | Data Protection Authorities should increase cooperation between each other to ensure the functioning of the "one-stop-shop", including sharing information on cross-border cases and providing support to each other during investigations. |
| **USE THE URGENCY PROCEDURE** | Data Protection Authorities should start utilising the urgency procedure laid down in Article 66 of the GDPR to adopt temporary measures or to force other authorities to act. |
| **DO NOT MISUSE THE GDPR** | Data Protection Authorities hold much of the responsibility for the GDPR's success or failure. It is absolutely unacceptable that DPAs misuse the GDPR to undermine human rights, restrict freedom of the press, or otherwise stifle NGOs' work. |
| **UPHOLD DATA PROTECTION RIGHTS DURING CRISES** | When governments adopt emergency legislations and derogate from human rights obligations, national DPAs and the EDPB will have a crucial role in maintaining scrutiny over measures impacting data protection. In the context of the COVID-19 crisis, the DPAs must uphold the GDPR and provide guidance to states. |

# CONCLUSION

The first two years of the GDPR has been a time of crises, whether internal, external, political, geopolitical, or administrative. In this sense, its early life has had much in common with the negotiating phase of the law. At the time, lawmakers in Brussels faced an unprecedented amount of lobbying designed to undermine the GDPR.

Since its adoption, the law has been seen worldwide as one of the major successes of the EU and one of the most robust frameworks for the protection of fundamental rights globally. But the lobbying to undermine the GDPR has not stopped, and the crises continue unabated. While the GDPR has so far resisted challenges and the content of the law does not require reform, its application and enforcement remain problematic.

Crippled by a lack of resources, tight budgets, and administrative hurdles, Data Protection Authorities have not yet been able to enforce the law adequately. Worse, some public authorities have misused the GDPR to undermine other fundamental rights. While the GDPR in itself is not to blame for these failures, fingers are sure to be pointed at the law if urgent actions are not taken. We hope that the recommendations put forward in this report will help address the situation.

It is now time to act and enforce the law as the world watches and the GDPR continues to serve a global standards-setter for data protection. We should not underestimate the importance of getting the enforcement of the GDPR right for businesses and users in the EU, and for the positive impact on data protection and human rights beyond the EU borders.

**For more information, visit our Data Protection page:**

**https://www.accessnow.org/issue/data-protection/**