



ONE YEAR UNDER THE EU GDPR

AN IMPLEMENTATION PROGRESS REPORT

State of play, analysis, and recommendations



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, and convenings such as RightsCon, we fight for human rights in the digital age.

This report was prepared by Estelle Massé and Laureline Lemoine.

For more information, please visit: <https://www.accessnow.org>

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

This report is an Access Now publication.

EXECUTIVE SUMMARY

It has been a full year since the EU General Data Protection Regulation (GDPR) entered into application. In the past 12 months, we have witnessed the first positive impacts of the law but also its struggles. People living in the EU have been using their rights to access data, erasure, object, withdraw consent, and more; a large number of complaints have been filed in front of the authorities; and the data protection authorities (DPAs) have slowly started enforcing the law by applying the first fines. In this report, we look back at the implementation of the GDPR since its adoption in May 2016 and entry into application in May 2018. 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.

Access Now has researched how the GDPR has been implemented in the 28 EU Member States around key measures for users' rights and we present the results in this report. Based on these findings, we have laid out recommendations to ensure that the rights and protections encompassed under the GDPR are effectively delivered to data subjects across the EU. These recommendations are addressed to EU Member States and their national DPAs, as well as for the EU Commission and the European Data Protection Board (EDPB).

Despite the two-year period for the implementation of the GDPR between 2016 and 2018, at the time of our report three Member States have yet to adopt national legislation adapting the law. In addition, several Member States have broadly interpreted the derogations, exceptions, and restrictions available under the GDPR which may create fragmentation in the level of protection for data subjects across the EU. In the worst cases, a small number of Member States have adopted national measures that are contradicting the spirit, objective, and text of the GDPR. We urge the EU Commission to use its powers under the EU treaties to intervene in countries where national measures, actions, and decisions undermine the core purpose of the GDPR at the expense of people's rights.

In this report, we looked in detail at the adaptation and implementation of eight key GDPR provisions in Member States. These provisions concern the age of children's consent, rules on automated decisions making, general restrictions to rights provided under the GDPR, measures on data breaches, possibilities for users to bring complaints, derogations for research purposes, and the functioning and powers of DPAs.

For each issue, we have identified risks of fragmentation and put forward recommendations to ensure that access and interpretation are harmonised across the EU. We for instance make recommendations to Member States to ensure that their respective national adaptation law is in line with the GDPR, to the EU Commission to intervene in cases where users' rights are being restricted as the result of poor implementation of the GDPR, to DPAs to prioritise the processing users' complaints, and to the European Data Protection Board to ensure cooperation between authorities and transparency in discussions and proceedings.

The GDPR will only be as strong as its weakest link and it is crucial to address any implementation issue early on to avoid crippling the benefits the law can bring to users. In the digital era, the relevance and importance of the GDPR in Europe and beyond has been well established.

While the nearly five years of GDPR negotiations have been challenging, its adoption is only a first step and victory in the effective delivery of strengthened data protection rights in the EU, and the biggest challenges lie ahead. After a first year of application, the law will now need to deliver its promises consistently through proper implementation and enforcement. Much of this responsibility now lies with the data protection authorities who will need to act swiftly and in a coordinated manner. Despite the central role given to DPAs, Member States are currently failing to provide adequate funding or staffing for these authorities so that they can effectively perform their tasks. In this report, we make recommendations to address this issue and ensure the independence of the DPAs.

With long-term investment and commitment from the EU Commission, the Member States, and DPAs, and the help of civil society, the GDPR has the potential to be one of the EU's greatest successes in the protection of fundamental rights.

See an error? Please contact us!

The information for this report was collected from 28 different national laws in nearly all 22 EU official languages. While we did our best to use official sources and translations when available, this report may contain errors or inaccuracies due to translation issues and/or linguistic misunderstanding.

We welcome and encourage your feedback and corrections. Please contact us at:
estelle@accessnow.org

TABLE OF CONTENTS

| | |
|--|-----------|
| EXECUTIVE SUMMARY | 2 |
| INTRODUCTION & METHODOLOGY | 5 |
| GDPR IMPLEMENTATION IN THE EU MEMBER STATES | 7 |
| CHILD’S AGE OF CONSENT (ARTICLE 8 GDPR) | 7 |
| AUTOMATED INDIVIDUAL DECISION-MAKING (ARTICLE 22 GDPR) | 8 |
| RESTRICTIONS (ARTICLE 23 GDPR) | 15 |
| NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY AND THE DATA SUBJECT (ARTICLES 33 AND 34 GDPR) | 18 |
| POWERS OF SUPERVISORY AUTHORITIES (ARTICLE 58 GDPR) | 20 |
| REPRESENTATION OF DATA SUBJECTS (ARTICLE 80(2) GDPR) | 28 |
| PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC, OR HISTORICAL RESEARCH PURPOSES, OR STATISTICAL PURPOSES (ARTICLE 89 GDPR) | 29 |
| EVALUATING PROGRESS: MORE WORK IS NEEDED TO PROTECT USERS’ RIGHTS AND CHANGE BUSINESS BEHAVIOUR | 33 |
| ROOM FOR IMPROVEMENT | 33 |
| THE ROLE OF DATA PROTECTION AUTHORITIES | 34 |
| THE RISK OF “BUSINESS AS USUAL” | 35 |
| “THE WHOLE WORLD IS WATCHING US” | 36 |
| RECOMMENDATIONS: MOVING THE GDPR APPLICATION AND ENFORCEMENT FORWARD | 38 |
| 1. RECOMMENDATIONS TO MEMBER STATES | 38 |
| 2. RECOMMENDATIONS TO THE EU COMMISSION | 38 |
| 3. RECOMMENDATIONS TO THE NATIONAL DATA PROTECTION AUTHORITIES | 39 |
| 4. RECOMMENDATIONS TO THE EUROPEAN DATA PROTECTION BOARD | 39 |
| CONCLUSION | 40 |
| ANNEX - GDPR NATIONAL ADAPTATION LAWS | 41 |

INTRODUCTION & METHODOLOGY

On 25 May 2018, the General Data Protection Regulation entered into application in the European Union.¹ A year later, we are evaluating the impact it has had so far on users' rights and we seek to identify the challenges ahead.

For this report, Access Now looked at how Member States are implementing the GDPR and using derogations, exceptions, and restrictions provided under the law. The GDPR is a Regulation, meaning that all provisions should be directly applicable in all Member States. However, the law includes a series of provisions that allow EU countries to establish legal measures that deviate, derogate, or interpret certain rules. We looked at how Member States have implemented eight key derogations of the GDPR into their national law:

- **Child's age of consent (Article 8)**
- **Automated individual decision-making (Article 22)**
- **Restrictions (Article 23)**
- **Notification of a personal data breach to the supervisory authority and the data subject (Articles 33 and 34)**
- **Powers of supervisory authorities (Article 58)**
- **Representation of data subjects (Article 80.2)**
- **Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89)**

While Member States can use other derogations and exceptions under the GDPR, we chose to focus on these due to their relevance to users' rights.

We did this by reviewing the national laws of all 25 countries having implemented the GDPR at the time of the report. We also analysed the draft laws for Portugal, Slovenia, and Greece, which are still in the process of ratifying their national adaptation law. For each law or draft, we looked at the text in their original language or the English version when it exists. We provide links to the laws we analysed in the annex of this report.

One of our goals in undertaking this research is to determine how easy it is to find information regarding data subject rights, given that national laws impact these rights through their implementation of flexibilities from the GDPR. We searched national laws by titles and chapter, using key words relating to these rights, as written in the corresponding GDPR provision, just as non legal-literate users would do. For some provisions, academics and NGOs had already done research, and we used and referred to their work to confirm our findings.

¹ See 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), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

In this report, when we say that Member States did not deviate from the GDPR, it means that they did not make use or refer to a specific derogation, exception, or restriction in the national adaptation law. When we say that a Member State has deviated from the GDPR, it means that it has used one or more of such provisions under the GDPR and added details or conditions about it in their national law.

We have further analysed the work of DPAs and the EDPB and looked at the behaviour of large tech companies and reactions by users since the law became applicable. This research was conducted through reading academic articles, official reports from authorities, and news articles. This research did not, however, include consultation with stakeholders, interviews with data subjects, or review of complaints.

From the findings we draw based on this research and analysis, Access Now has developed recommendations for Member States, the EU Commission, DPAs, and the EDPB to follow in order to overcome the obstacles that may cause fragmentation and could undermine the protection of the fundamental right to data protection across the EU.

I. GDPR IMPLEMENTATION IN THE EU MEMBER STATES

CHILD'S AGE OF CONSENT (ARTICLE 8 GDPR)

Article 8 of the GDPR requires that parental consent be obtained for information society services offered directly to a child under the age of 16. Member States may provide by law for a lower age for those purposes, provided that such lower age is not below 13 years.

Children's right to data protection can be put at risk when their personal information is collected, stored, or processed. Children's capacity to make decisions about their personal data protection rights can be affected by measures that restrict access to information, inhibiting their ability to make choices in line with their developing capacities.² There is a need for additional measures to protect children's rights. As the Article 29 Working Party noted, the GDPR does not specify practical ways to get the parent's consent or to establish that someone is entitled to perform this action.³ Without efficient age verification in place and with diverse ages of consent throughout Member States, the GDPR does not properly assess the reality of children's activity online and does not therefore provide appropriate protection.

The possibility for derogation introduced in the GDPR has led to fragmentation in the definition of the age of consent for children across the EU as can be seen in the map presented below. Research shows that children must be given a certain degree of autonomy to help them grow and develop maturity. The fragmentation in the definition of the age of consent may create differences across the EU in development and responsibility of children based on the degree of independence they have. Additionally, cross-border services will be faced with operational challenges despite the promise of the GDPR to deliver "one law for one continent".

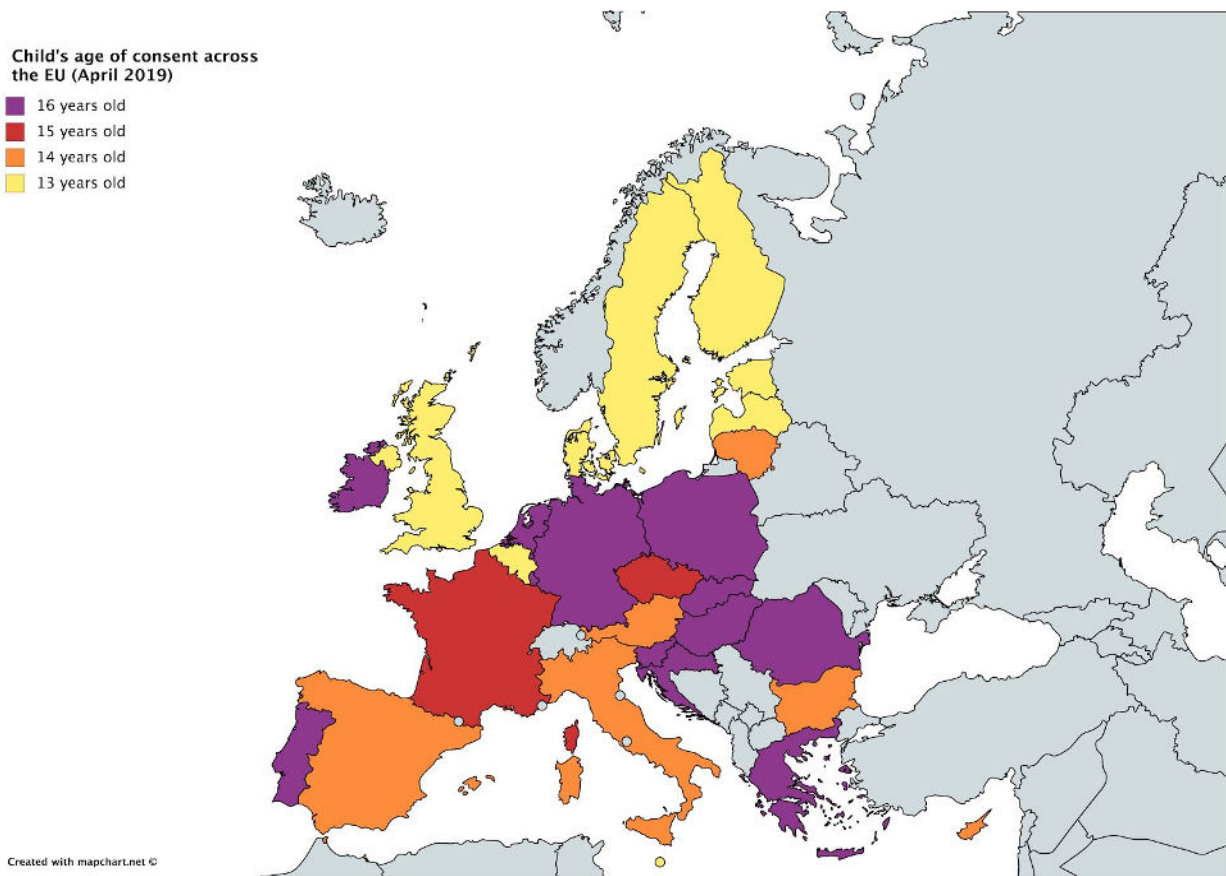
→ We found that **16 Member States** chose to use the possibility provided under Article 8 to lower the age threshold.⁴

It should be noted that this information is **subject to change** as some Member States have not implemented the GDPR yet. The legislative procedure is still pending in Greece, Portugal, and Slovenia. As of May 2019, the age of consent in these three Member States is set to 16 but the **draft laws show that they all intend to lower this age to 15** for Greece and Slovenia and 13 for Portugal.

² See UNICEF's Toolkit "children's online privacy and freedom of expression", 2018, available at [https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf).

³ See Article 29 Working Party's guidelines on Consent under Regulation 2016/679, 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

⁴ See "Counting down to 25 May 2018: mapping the GDPR age of consent across the EU (May 2018)", I. Milkaite and E. Lievens, Ghent University, available at <https://biblio.ugent.be/publication/8561253/file/8561256.pdf>.



Map 1. Child's age of consent for data processing across the EU (April 2019)

AUTOMATED INDIVIDUAL DECISION-MAKING (ARTICLE 22 GDPR)

Article 22 of the GDPR provides that a “data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning individuals or similarly significantly affects them”.

Under this article and corresponding recitals, data subjects have two different protections:

1. the right to know about the existence of an automated processing and to receive meaningful information about its logic, significance, and consequences.
2. the right not to be subject to that processing, unless in specific cases (pre-contractual or contractual context, explicit consent of data subjects, Member States or EU law exemptions where suitable measures to safeguard users' rights must be provided).

Under Article 22(2), b, Member States can adopt laws that obviate the application to the right to not be subject to automated decision-making. If they decide to do so, they also must lay down “suitable measures to safeguard the data subject's rights and freedoms and legitimate interests”.

The scope of Article 22 is quite narrow as it only encompasses “decision based **solely** on automated processing”, leaving out semi-automated decision-making used for example as decision support.⁵ Moreover, the interpretation of “solely” is being discussed and might required further explanation by the European Court of Justice.⁶

- We found that **19 Member States** did not use the derogation in Article 22(2)b. in their national data protection laws. This means that the application of the right for users to not be subject to automated decision-making as defined under Article 22 remains untouched. These Member States are: Italy, Romania, Sweden, Denmark, Poland, Finland, Cyprus, Greece, Czech Republic, Estonia, Lithuania, Bulgaria, Latvia, Portugal, Croatia, Slovakia, Luxembourg, Malta, and Spain.

However, it cannot be excluded that these Member States might in fact make use of this derogation in future legislation outside of their national adaptation law.

- In contrast, **nine Member States** have used the provision in Article 22(2).b to obviate users’ right to not be subject to automated decision-making and have explicitly regulated automated decision-making: Austria, Belgium, France, Germany, Hungary, Ireland, Slovenia, The Netherlands, and the UK.

The use of this derogation by nine Member States creates a risk of fragmentation across the EU and raises implementation issues. Indeed, what will happen if data from individuals in one Member State are used in another Member State by public and private sector controllers and these two States do not have the same rights and safeguards around automated decision-making and profiling, including the right to not be subject to such processing? This has implications for access to jobs, healthcare benefits, education, and more, as national employment agencies, university admissions, and public health institutions are increasingly relying on automated decision-making processes.

It is interesting to note that Member States have laid down specific measures to obviate the application of a user’s right to not be subject to automated decision-making on two main issues:⁷

- (i) the issue of **when** the right is limited, that is, in which case the use of automated decision-making cannot be opposed by users;
- (ii) the issue of **how** it is regulated, that is, which safeguards the Member States propose when a user’s right is being limited pursuant this Article.

Regarding the scenarios under which Member States have established that the **USE OF AUTOMATED DECISION-MAKING CANNOT BE OPPOSED** by users pursuant Article 22(2) b., there are four different approaches:

⁵ See “Slave to the algorithm? Why a ‘Right to an explanation’ is probably not the remedy you are looking for”, L. Edwards; and M. Veale, 2017, available at <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1315&context=dltr>.

⁶ See ICO, Feedback request –Profiling and automated decision-making [v 1.0,2017/04/06] (2017) at 20, <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>.

⁷ See “Automated Decision-Making in the EU Member States: The right to Explanation and other ‘suitable safeguards’”, G. Malgieri, 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233611.



Provides for **sectorial exceptions**, notably in the insurance context. Automated decisions can be used without individual consent and appeal mechanisms if the individual's request is granted (e.g., receives the full value of a claim). If the request is denied, suitable safeguards must be provided. For health insurance, no prior consent is necessary for automated decisions based on binding fee-for-service tables for medical procedures — but the insurer must inform the individual (at the time of full or partial denial) that a human appeal mechanism is in place.



Refers to **exceptions based on specific legal bases** for data processing as described at Article 6 of the GDPR, in particular legal obligation and public task: “if the automated decision-making [...] is necessary to comply with a legal obligation resting on the controller or necessary for the fulfilment of a task of general interest”.



These countries provide **general reference to other national laws** that would justify the limitation on the right to not be subject to automated decision-making:

- Austria: automated decisions “are permitted only where expressly provided for by law or by directly applicable legislation having the status of a national law”.
- Belgium: automated decision-making is permitted “if the law, decree, ordinance, act of the European Union or international agreement provides appropriate safeguards”.
- Hungary: automated decisions “may only be made if it expressly permitted by law or by a mandatory legal act of the European Union”.
- Ireland: “if they are authorised or required by or under an enactment”.
- Slovenia: “unless expressly permitted by a law which also provides for appropriate measures”.



These countries adopted a **general approach obviating the application of users' right to not be subject to automated decision making, but only if certain safeguards and conditions are met:**

- France: The use of automated decision-making is always allowed, and a user cannot exercise a right not to be subject to this processing. However, judicial decisions

based on automated means are prohibited. Similarly, administrative decisions based on automated means are only permitted under certain conditions.

- Decisions which have “legal effects or significant effects on a person”, based on automated means are allowed without possibility for the data subject to not be subject to this processing provided that the rules defining the data processing and the main features of its implementation are communicated to the data subject, with the exception of secrets protected by law, by the data controller to the person concerned, upon her/his request.
- The UK: The use of automated decision-making is always allowed, and user cannot exercise a right not to be subject to this processing. However, the country set up a list of safeguards to follow “where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing: [...]”.

Regarding the **SAFEGUARDS** proposed by Member States when the right to not be subject to automated decision-making is being restricted:

When applying Article 22(2) b., Member States could implement the three minimum safeguards required by Article 22(3):

1. the right to obtain human intervention on the part of the controller,
2. to express his or her point of view, and
3. to contest the decision.

Recital 71 of the GDPR also mentions a **right to an explanation**. But as well as only being mentioned in a recital, it is not clear what this right precisely entails. Is it a right to obtain information on the architecture of the algorithm, the implementation of the algorithm, or both? With no clear answer in the GDPR, this matter is left to the interpretation of the DPAs, the courts, and to the Member States that will implement this right. At this stage, it is not clear how this general right can be implemented in practical cases and whether it will be feasible for each kind of individual automated decision.⁸ So far it is expressly referred to in legislation in France and Hungary without being defined in detail.

Member States have different approaches and propose different safeguards in response to their obligation to introduce “suitable measures to safeguard the data subject's rights and freedoms and legitimate interests” under Article 22(2)b.:

⁸ See “Automated Decision-Making in the EU Member States: The right to Explanation and other ‘suitable safeguards’”, G. Malgieri, 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233611; See “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, S. Watcher; Brent Mittelstadt; and Luciano Floridi, International Data Privacy Law, 2017, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469.; See Access Now’s report - “Mapping artificial intelligence strategies in Europe”, available at https://www.accessnow.org/cms/assets/uploads/2018/11/mapping_regulatory_proposals_for_AI_in_EU.pdf.



These countries simply **recite the rights provided in Article 22(3)**, which are “the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.” They do not provide extra rights to data subjects.



These countries go further and elaborate on the **right to explanation**, though the right is only granted upon request by the data subject.

In Hungary the data controller should inform the subject about “the **methods and criteria** used in the decision-making mechanism”. It is not clear whether this involves the algorithm architecture (i.e., the ex ante information about the functionality of the algorithm) and/or the algorithm implementation (i.e., ex post explanation on the practice of the algorithm in a given case).

The French law is more clear and expressively recognises a right to an explanation of both the **architecture of the algorithm** and the **individual decision**.

For *administrative decisions*, the data controller must ensure the control of the algorithmic processing and its evolution in order to be able to explain, in detail and in an intelligible form, to the person concerned how the processing has been implemented in his respect.



These countries have a more **general and procedural approach**, regulating the potential requests of data subjects regarding automated processing and the possible reactions of the data controller (e.g., what alternatives processing could be offered, etc.).

In the UK, data subjects have a right to receive notification of automated decision-making, which must be provided “as soon as reasonably expectable”.

In the UK and in Ireland, data subjects have then a right to contest automated decision (through human intervention or reconsideration) and, in response to this contestation, they have a right to receive information on the steps taken, compliance, and the outcome of the decision.



Requires data controllers to conduct a **Data Protection Impact Assessment** (DPIA) on algorithmic decision-making systems to identify, assess, and mitigate the risks of a system before it is used. The law explicitly says that this should be performed in order to protect human rights and freedoms of the data subject.

It is interesting to note that in all of these approaches, except for the Slovenian one, the **safeguards depend upon the data subject’s request, which means that the safeguards are dependent on data subjects expressly asking for it**. For instance, users have to actively request a human intervention or an explanation, which endangers the effectiveness of the safeguards if data subjects are not made aware of such possibility.

In the same way, a real right to human involvement only makes sense if it is then combined with a clear prior notification and a clear explanation of the decision to users when the data controller seeks to use automated decision-making.

The table below summarises the safeguards found in the GDPR and the safeguards Member States chose to implement when using the derogation provided for in Article 22(2)b.

| | Right to human intervention | Right to express his/her view | Right to challenge or contest a decision | Right to receive notification about automated decisions and related safeguards | Right to receive notification of the contestation outcome | Right to receive explanation on architecture or implementation of algorithms | DPIA on Automated Decision-making systems |
|--|-----------------------------|-------------------------------|--|--|---|--|---|
| Article 22(3) GDPR | ✓ | ✓ | ✓ | | | | |
| Recitals of GDPR | ✓ | ✓ | ✓ | | | ✓ | ✓ (implicit) |
|  Austria | ✓ | ✓ | ✓ | | | | |
|  Belgium | ✓ | | | | | | |
|  France | ✓ | ✓ | ✓ | | | ✓ | |
|  Germany | ✓ | ✓ | ✓ | ✓ | | | |
|  Hungary | ✓ | | ✓ | | | ✓ | |





| | | | | | | | |
|--|---|---|---|---|---|--|--|
|  Ireland | ✓ | ✓ | ✓ | | ✓ | | |
|  Slovenia | | | ✓ | | | | |
|  The Netherlands | ✓ | ✓ | ✓ | | | | |
|  The UK | ✓ | ✓ | ✓ | ✓ | ✓ | | |

Table 1. Different Safeguards for Automated Decision-Making proposed in the GDPR and in Member State Legislation

Finally, it is important to note that not all Member States define automated decision-making in the same manner in their national laws. This may impact the **SCOPE** of the derogation on the application of users' right to not be subject to automated decision-making. Member States follow three different approaches:

 **Germany**
 **Ireland**
 **The Netherlands**
 **The UK**

These countries refer to the **general definition of Article 22(1)**:

“decision based solely on automated processing, including profiling, which produces **legal effects** concerning him or her or **similarly significantly affects** him or her”.

This terminology will have to be further defined to ensure consistent implementation of measures related to automated processing. We for instance need clarity around what can be considered “significant”.

 **Austria**
 **France**
 **Hungary**

These countries have **extended the definition of Article 22(1) by introducing more vague wording.**

- Austria: “decisions based only on automated processing, including profiling, which have **detrimental consequences** for the data subject or that could **significantly affect** them”.
- “Detrimental consequences” is a lower threshold to reach than “legal effects”. The national law also refers to **any** significant effects, not only “effects which are *similarly significant*” as legal effect, like in Article 22(1).
- France: “a decision which has **legal effects or significant effects** on a person”

- This means *any* significant effects, not only effects which are as *similarly significant* as legal effect like in Article 22(1).
- Hungary: “decisions based only on automated data processing, in particular profiling, which are **prejudicial** to the person or **legitimate interests** of the person or which have a **significant impact** on the person concerned”
- “Prejudicial” and any “significant impact” is wider than “legal or similarly significant effects” . Moreover, the GDPR only mentions effects “concerning him or her” while the Hungarian law includes the person’s legitimate interests as well.



Slovenia

The draft law suggests a **narrower definition than Article 22(1) GDPR**.

“decisions based exclusively on automated processing of personal data, including profiling, that have **negative** legal consequences for the data subject or are *likely to affect them to a greater extent*”.

“Negative legal consequences” is a narrower scope than any “legal effects” in Article 22(1). Similarly, “to a greater extent” is a higher threshold than any “similar significant effects”.



Belgium

Belgium has adopted a definition that **is both wider in places** than the language provided for under Article 22(1) GDPR and **narrower in others**.

“any decision based exclusively on automated processing, including profiling, which produces **adverse** legal effects for the data subject or **significantly affects** him/her”.

This means *any* significant effects, not only effects which are as *similarly significant* as legal effect like in Article 22(1).

However “adverse legal effects” is a narrower standard than the general “legal effects” referred to in Article 22(1).

RESTRICTIONS (ARTICLE 23 GDPR)



Article 23 allows Member States to restrict the rights of data subjects provided for in the GDPR.













They can do so for different reasons, including national and public security, defense, objectives of general interests, the protection of judicial independence and proceedings, protection of the data subject or the rights and freedoms of others, or the enforcement of civil law matters. Such restrictions must respect the essence of the fundamental rights and freedoms and must be a necessary and proportionate measure in a democratic society.








The application of these restrictions by Member States remain largely **discretionary**, especially in relation to concepts like national or public security, which Member States can stretch and abuse. However, the safeguards (essence of fundamental rights, proportionality) mean that restrictions which are too broad could potentially be challenged in front of the European Court of Justice.








But because of these widely drafted restrictions, there is a **risk of loopholes** that could potentially **weaken the full force of the GDPR**.

Moreover, European citizens will have different rights restricted depending on the Member States:


























| | |
|---|---|
| Transparent information (Article 12 GDPR) | 1 Member State <div style="display: inline-block; vertical-align: middle; text-align: center;">  Cyprus </div> |
| Right to information (Article 13/14 GDPR) | 11 Member States <div style="display: flex; flex-direction: column; align-items: flex-start; margin-top: 10px;"> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Austria</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Belgium</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Denmark</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Estonia</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Finland</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> France</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Germany</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Hungary</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Luxembourg</div> <div style="display: flex; align-items: center; margin-bottom: 5px;"> Poland</div> <div style="display: flex; align-items: center;"> Slovenia</div> </div> |

| | | |
|---|-------------------------|---|
| <p>Right of access (Article 15 GDPR)</p> | <p>12 Member States</p> | <ul style="list-style-type: none">  Austria  Belgium  Denmark  Estonia  Finland  France  Germany  Hungary  Latvia  Luxembourg  Poland  Slovenia |
|---|-------------------------|---|

| | | |
|--|------------------------|--|
| <p>Right to rectification (Article 16 GDPR)</p> | <p>7 Member States</p> | <ul style="list-style-type: none">  Austria  Belgium  Estonia  France  Hungary  Luxembourg  Slovenia |
|--|------------------------|--|

| | | |
|--|------------------------|---|
| <p>Right to erasure (Article 17 GDPR)</p> | <p>7 Member States</p> | <ul style="list-style-type: none">  Austria  Belgium  Estonia  France  Hungary  Luxembourg  Slovenia |
|--|------------------------|---|

| | | |
|--|------------------------|--|
| <p>Right to restriction of processing (Article 18 GDPR)</p> | <p>3 Member States</p> | <ul style="list-style-type: none">  Cyprus  Hungary  Slovenia |
|--|------------------------|--|

| | |
|---|---|
| <p>Notification obligation (rectification or erasure or restriction of processing) (Article 19 GDPR)</p> | <p>2 Member States</p> <ul style="list-style-type: none">  Cyprus  Germany |
| <p>Right to data portability (Article 20 GDPR)</p> | <p>1 Member State</p> <ul style="list-style-type: none">  Cyprus |
| <p>Communication of data breach (Article 34 GDPR)</p> | <p>7 Member States</p> <ul style="list-style-type: none">  Austria  Belgium  Denmark  Estonia  France  Germany  Slovenia |
| <p>All the rights</p> | <p>10 Member States</p> <ul style="list-style-type: none">  Bulgaria  Croatia  Ireland  Italy  Malta  The Netherlands  Slovakia  The UK  Greece  Czech Republic |
| <p>No implementation or not found</p> | <p>5 Member States</p> <ul style="list-style-type: none">  Lithuania  Portugal  Romania  Spain  Sweden |

- Between the eight provisions we looked at, the restrictions listed under this Article are the most used, as **23 Member States** introduce restrictions based on it. **Ten Member States chose to restrict every right** mentioned but the others picked and chose among them. The use of such restrictions, either partly or fully, create a **fragmented and uncertain legal framework** for users' rights to data protection in the EU.

Regarding the **five Member States** that did not implement Article 23, it is possible that such restrictions could be found in other laws Access Now did not review for this report. It is indeed common to find these restrictions not in the national laws implementing the GDPR but in other national legislation on defense, security, finances, and more. This makes the mapping and analysis of such restrictions difficult, in particular when conducted in more than 20 languages, and in countries with different approaches to procedural and/or criminal law. This is an issue, not just for researchers and experts, but also for **data subjects who may not have legal literacy**, and therefore might not know whether or how their rights are being restricted. The EU Commission would be well-placed to conduct such a mapping for the 2020 implementation report on the GDPR in order to evaluate the extent of the use by Member States of the restrictions provided for under Article 23.

NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY AND THE DATA SUBJECT (ARTICLES 33 AND 34 GDPR)

Article 33 requires that, in the case of a breach, the controller notifies the breach to the **supervisory authority** without undue delay and, where feasible, not later than 72 hours after having become aware of it. When a controller notifies a breach to the supervisory authority, Article 33(3) specifies the minimum communication requirements, such as describing the nature of the breach, the consequences, and measures taken to address it.

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases in paragraph four, recognises that a controller may not always be able to notify a breach to the authority within that time period, and that a delayed notification may be permissible.

In certain cases, as well as notifying the supervisory authority, the controller is also required to **notify the affected individuals**.

Article 34(1) states: “When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay”.

When notifying individuals, Article 34(2) specifies that: “The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)”.

As no system is completely secure, mandatory breach notifications are effective to force organisations to quickly and actively address breaches. Notification to users can be essential in helping individuals to regain control of personal information that has been compromised. Every data subject has a right to know that their data has been compromised and to know who has the capacity to keep their data secure.

Despite this, Article 23 GDPR allows for a **restriction regarding Article 34**, which means that controllers might be **exempted from communicating a breach to the affected individuals**.

- This restriction was dealt with in relation to Article 23 where we saw that **seven Member States chose to implement it**. These Member States are: Austria, Belgium, Denmark, Estonia, France, Germany, and Slovenia.

Apart from implementing this restriction, Member States can choose to **deviate** from both Article 33 and 34, which means that they can modify, add, or delete requirements and exceptions when implementing these articles into their national legislation.

- **Twenty Member States chose to not deviate from Article 33 and 34**, which means that data breaches need to be notified to the supervisory authority under 72 hours and without undue delay to the data subjects.
 - ◆ These Member States are: Belgium, Croatia, Denmark, Czech Republic, Estonia, Finland, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, and Spain.
- **Eight Member States** chose to **deviate from the GDPR**, by **adding further exceptions** to the notification of breaches (other than the ones in Article 23 of the GDPR) or by **modifying or specifying** the requirements of notification of Articles 33 and 34 as follows:



adds **two exceptions to the notification of breaches**:
(1) for the protection of the constitutional institutions of the Republic of Austria, and
(2) for the protection of military intrinsic security.



defines the meaning of “without undue delay” in Art. 34: it means seven days. The data administrator shall notify the data subject about the breach, not later than seven days after its establishment, whereas in the GDPR, the data controller must notify “without undue delay”.



It is a **criminal offense**
(1) not to notify the Supervisory Authority about a data breach (Article 33 GDPR), and
(2) not to notify the data subject about a data breach (Article 34 GDPR).



replaces the 72 hours delay for Article 33 with “without delay” but without defining a timeframe or providing guidance on how to interpret this language.



(1) adds an exception if the obligation under Article 34 GDPR would disclose **information which by law or by its nature must be kept secret**, in particular because of **overriding legitimate interests of a third party**. By derogation from this exception, the data subject shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage;

(2) specifies that breach notifications made to DPAs or individuals cannot be used as evidence in fining procedures against the notifying organisation without its consent.



adds an exception regarding undertakings offering **financial services** (as defined by the Act on Financial Supervision (Wet op Financieel Toezicht)) which are not under the obligation to notify the data subject of a data breach.



adds an exception regarding Articles 33 and 34 which do not apply in the case of personal data incidents to be reported in accordance with the Security Protection Act (2018: 585) or regulations that have been notified in connection with that law.



adds **several exceptions** to Article 33, such as when:

- (1) the data breach also constitutes a relevant error within the meaning of Section 231(9) of the Investigatory Powers Act 2016 (Clause 106(6) UK Bill);
- (2) information is required to be disclosed to the public by law;
- (3) there is infringement of parliamentary privilege;
- (4) Crown honours and dignities are at risk; and
- (5) negotiations with the data subject.

There is also no notification obligation when the personal data concerned relates to:

- (6) confidential references by the controller;
- (7) exam scripts and marks (Schedule 11 UK Data Protection Act 2018). It is required to communicate the nature of a data breach

to the data subject (Clause 68(2)(a) UK Data Protection Act 2018).

POWERS OF SUPERVISORY AUTHORITIES (ARTICLE 58 GDPR)

The national data protection authorities have a central role in the application of the GDPR as they **provide guidance and enforce the law**. They monitor the activities of data controllers and processors to ensure that they comply with their obligations and play a key role in investigating violations of rights. For these authorities to be able to function properly and efficiently, it is important that Member States provide them with **sufficient financial and human resources**. The national authorities need to be able to deal with breach notifications and to have means to investigate. They are the key to the success - or the failure - of the enforcement of the GDPR.

Below, Access Now looked at the additional powers some Member States chose to include in their national legislation as well as the issue of the national authorities' resources and their enforcement power through fines.

1. ADDITIONAL POWERS

Article 58 relates to the powers given to supervisory authorities. These powers are divided in three categories: investigative powers, corrective powers, and advisory powers.

Member States are allowed to give additional powers to their national authority according to Article 58(6).

- It seems that **17 Member States** chose not to provide additional powers to their data protection authorities. These are: Austria, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Luxembourg, Malta, Portugal, Romania, Slovakia, Slovenia, Sweden.

These or other Member States might add powers through a future law or may have already done so through a more specific legislation that Access Now is not aware of.

- At least **11 Member States** explicitly included additional powers to their national authorities or added details :

 **Belgium**

added investigative powers:

- (1) written and oral interrogations;
- (2) consulting IT systems and copying all data on these systems;
- (3) consulting information electronically;
- (4) seizing or sealing IT systems or goods; and
- (5) claiming the identification of a subscriber or usual user of an electronic communications service or of the used means of electronic communications.



Cyprus

added powers to:

- (1) access any personal data requested for any reason without any confidentiality claim (excluding the client-lawyer legal privilege);
- (2) dawn raid in any establishment (excluding houses);
- (3) engage forensic experts and/or the police forces for any of its functions;
- (4) confiscate any relevant documents and equipment;
- (5) impose conditions on a number of GDPR functions; and
- (6) report to the police and the criminal prosecutor any noncompliance that may amount to a criminal offense.



Germany

added details regarding the exercise of powers: If the Federal Commissioner concludes that data protection legislation has been violated or that there are other problems with the processing of personal data, he or she shall inform the competent authority for legal or technical matters and, before exercising the powers referred to in Article 58 (2) (b) to (g), (i) and (j) of the GDPR, shall give this authority the opportunity to provide its opinion to the controller within a reasonable period.



Ireland

the authority can appoint “authorized officers” at its own discretion who can exercise investigative powers broader than the ones in Article 58, similar to the ones added in other Member States.



Latvia

added investigative powers to visit State administration institutions and production facilities, warehouses, commercial, and other non-residential premises owned, possessed, or used by legal and natural persons in the territory of Latvia in order to verify conformity of the operation of the controller to the requirements of laws and regulations within the scope of its competence.



Lithuania

added the powers to obtain, free of charge, all necessary information, copies of documents and copies of data, copies of data and documents from controllers and processors, state and municipal authorities and bodies, as well as access to all data and documents necessary for the performance of the tasks of the supervisory authority functions.



The Netherlands

added the power to act against EU decision on transfers: in the context of an investigation of data transfers initiated by an interested party, the Dutch supervisory authority is competent to act against an adequacy decision or a decision establishing standard contractual clauses taken by the European Commission by filing a request with the Council of State to check on the decision's validity.



Poland

added the investigative powers to enter any land, buildings, premises, or other spaces. The inspector may also question the inspected party's employees as a witness.



Spain

added the investigative power to carry out searches on (private) homes in accordance with procedural rules governing these searches (e.g., upon prior judicial authorisation). They specified that the authority may also carry out preventive audits. Furthermore, the president of the authority will have the power to issue implementing legislation called "circulars" that will become binding after publication in the Official Gazette.



The UK

Powers are subject to information or enforcement notice.

On paper, these powers seem to be a positive addition to the ones already provided for in the GDPR. However, given that some powers are **far-reaching**, such as investigative powers to search private homes, Member States must ensure that the national authorities act with **complete independence** in performing their tasks and exercising these powers to avoid the risk of abuse thereof.

2. RESOURCES OF DATA PROTECTION AUTHORITIES ("DPA")

Under Article 52(4), the Member States are required to "ensure that each supervisory authority is provided with the **human, technical and financial resources**, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board".

On 26 February 2019, the European Data Protection Board ("EDPB") Chair and Vice-Chair addressed the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) on GDPR implementation and published a report providing a first overview of the implementation of the law.⁹

⁹ See "First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities", EDPB, 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

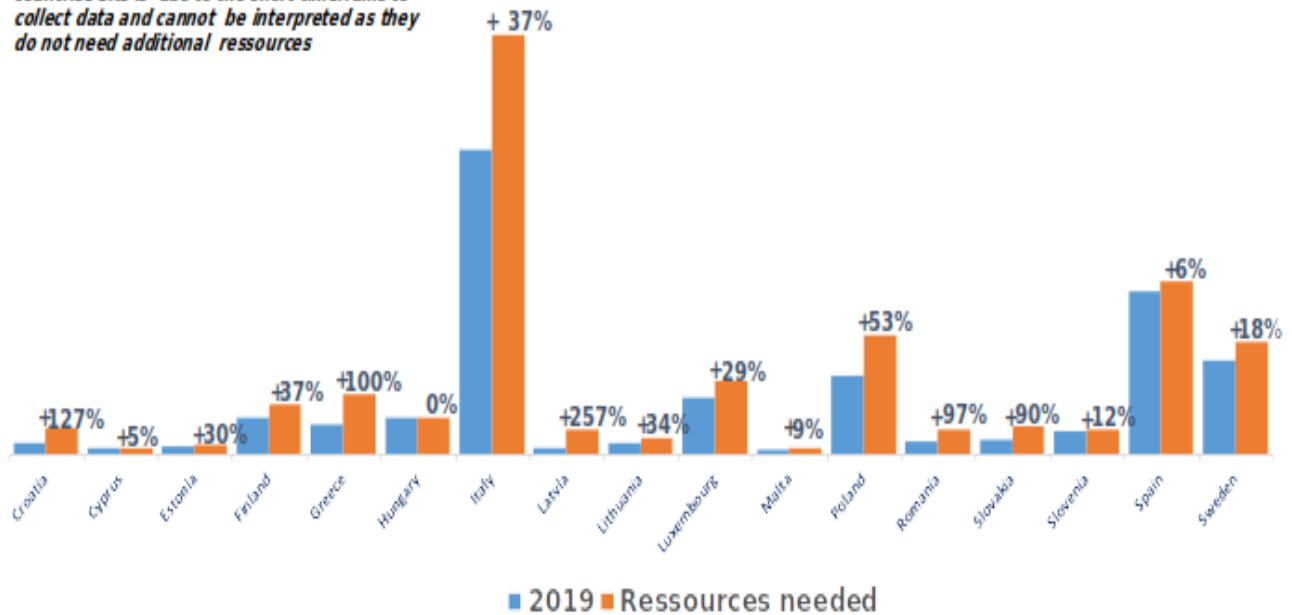
FINANCIAL RESOURCES

It was reported that, in most cases, there was an increase in the budget for 2018 and 2019, while, for the **Czech Republic** and **Poland**, a decrease was observed. In Austria, Belgium, and Latvia, no changes in the budget were noticed. According to information provided by the respective DPAs, the latter phenomena can be explained by biannual budget plans for this period of time.

The majority of the 17 replying DPAs stated that they would need an increase in the budget of 30-50%, but almost none of them received the requested amount. There are some extreme examples where this need is close to, or even above, 100%, like in **Latvia** (257%), **Croatia** (127%), **Greece** (100%), **Romania** (97%), and **Slovakia** (90%).

Budget needed vs Budget received

The missing information from some EEA countries SAs is due to the short timeframe to collect data and cannot be interpreted as they do not need additional resources



Based on information provided by SAs from 17 EEA countries

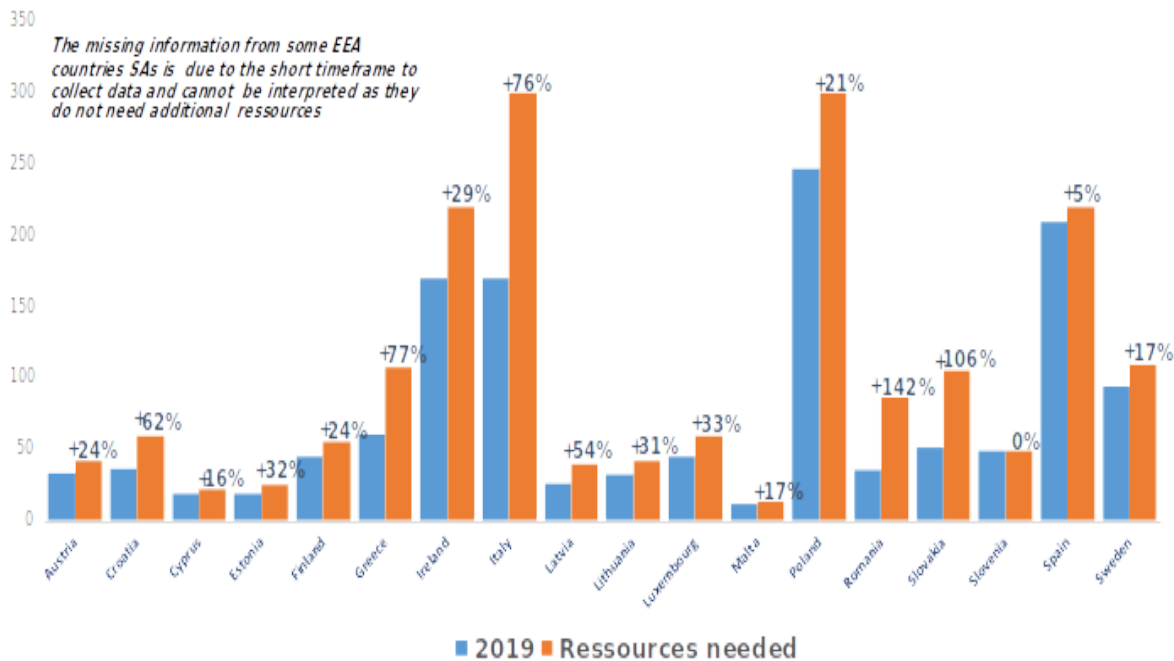
Source: [EDPB report - First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities](#)

HUMAN RESOURCES

Based on information provided by DPAs from 26 countries in the European Economic Area (“EEA”) and the EDPS, the majority of them have experienced an increase in the number of staff, while for **Austria**, **Bulgaria**, **Estonia**, **Italy**, **Latvia**, **Lithuania**, **Malta**, and **Romania**, the human resources did not change.

For the **Czech Republic**, there was even a decrease in personnel (-5%). **Almost all the replying DPAs** stated that they would need an increase of human resources ranging from 5% to 76% for **Italy**.

Number of employees needed vs Current number of employees



Based on information provided by SAs from 18 EEA countries

Source: [EDPB report - First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities](#)

National authorities lacking budget or human resources **cannot fully provide their citizens with the adequate data protection** offered by the GDPR. Moreover, the disproportion between the human and financial resources allocated in different Member States can **compromise the effectiveness of the one-shop rule**.

Ultimately, this can also **endanger the national authorities' independence** required under the GDPR. There is pressure coming from the fact that the Member States often provide for their budget, which could result in potential threats to cut funding over the authority's actions. Moreover, the issue of independence goes beyond this funding issue in Member States where the head of the authority is chosen by the government, even if this is authorised by the GDPR.

Issues related to independence already arose in **Romania**, where the national DPA asked journalists for information about "the sources from where the personal data was obtained" in relation to a state corruption case they covered.¹⁰ The DPA explicitly used the GDPR as a tool to force journalists to reveal their sources, mentioning a possible penalty of up to €20 million if the journalists didn't comply with its request, including a possible fine for "access to the data" under Article 83 (5) e) of the GDPR. This happened despite the fact that this was contradicting both the GDPR and the national implementing law. This issue is particularly troubling and shows why the independence of the DPA is so important and necessary.

3. FINES

¹⁰ See "GDPR misuse in Romania: 'independence of DPA' and 'transparency' – keywords or buzzwords?", GDPR Today, 2018, available at: <https://www.gdprtoday.org/gdpr-misuse-in-romania-independence-of-dpa-and-transparency-keywords-or-buzzwords/>.

Under Article 58(2)i, DPAs shall have the power to “to impose an **administrative fine** pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case”.

The Dutch regulator was the first to issue a fining policy, setting up categories of infringements and factors to be taken into account when imposing a fine.¹¹ As there is no harmonisation regarding fines, other Member States might choose to align with the Dutch policy or issue one of their own.

Companies have needed time to comply with the GDPR across the two-year implementation period and national regulators also needed to prepare for the thousands of complaints that have been filed. But **now it is time for the GDPR enforcement to grow some teeth**. Enormous data breaches appear to be increasing and the number of complaints being filed continues to increase.¹²¹³ Data protection authorities must not hesitate to enforce the GDPR through investigations and adequate fines so the full capabilities of the law can be realised.

Most fines imposed in 2018 have been under the pre-GDPR regime which means that regulators impose much lower fines than what is possible under the GDPR.

Thirteen data protection authorities imposed or recommended a fine, including Austria, Bulgaria, Cyprus, Denmark, France, Germany, Hungary, Italy, Malte, Poland, Portugal, and recently Lithuania and Belgium.

It is important to note that neither the legal system of Denmark nor that of Estonia allow for administrative fines. Therefore, national authorities can only recommend that a fine be imposed, while the national courts are the ones issuing it. This could potentially hinder enforcement of the GDPR as there is no way to make sure that the national courts will follow the authorities’ recommended fines. The procedures would also take longer. Moreover, it could create a forum-shopping issue if it turns out that this enforcement tool cannot be used.

Law firm DLA Piper reports that so far, **91 fines have been imposed under the GDPR**. Here are some **examples** of the (publicly available) fines issued as of May 2019:¹⁴

- The highest fine was imposed by the [French data protection authority, the Commission Nationale de l'Informatique et des Libertés \(CNIL\)](#) against Google for €50 million for the processing of personal data for advertising purposes without a valid authorisation.

¹¹See “Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019)”, Dutch Data Protection Authority/Autoriteit Persoonsgegevens. Available at <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586.pdf>.

¹² See DLA Piper GDPR data breach survey: February 2019, available at <https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/>.

¹³ See “The GDPR in numbers”, EU Commission, 2019. Available at https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers.pdf.

¹⁴ See GDPR enforcement tracker. Available at <http://www.enforcementtracker.com/#>.

- The German authority imposed 64 fines, including a €20,000 fine against a social network operator for failure to secure users' data and a €80,000 fine for publishing health data on the internet.
- The Italian Data Protection Authority has imposed its first fine for €50,000 for failure to implement adequate security measures after a data breach, against the Italian political party Movimento 5 Stelle.
- The Maltese authority imposed a total of 17 fines, including a €5,000 fine against the country's public property management department for failing to secure its website.
- Hungary imposed six fines, ranking from €1,500 to €34,500.
- The Portuguese authority imposed a €400,000 fine to a hospital where patients' information was inappropriately accessible by non-medical staff.
- The Austrian authority imposed a €5,280 fine against a sport betting café for unlawful video surveillance.
- The Polish authority imposed a €220,000 fine for the failure to fulfil the information obligation.
- Cyprus imposed four fines for a total of €11,500, including a €5,000 fine against a public hospital.
- The Bulgarian authority imposed a €27,100 fine to a telecommunication service provider for repeated registration of prepaid services without the knowledge and consent of the person concerned. Another €500 fine relates to a late and incomplete response to a request by an employee to access his own personal data.
- The Danish authority recommended a fine of 1.2 million kroner, approximately €160,754, against a taxi company for violating data retention periods.
- The Lithuanian authority has imposed an administrative fine of €61,500 to a company which improperly processed personal data in screenshots, made personal data publicly available and failed to report the personal data breach to the personal data protection supervisory authority.
- The Belgian authority has imposed a fine of €2,000 for abusive use of personal data for electoral campaigning purposes by a mayor.

It is interesting to note that across the EU fines seem to be imposed on public and private entities and on small businesses as well as big tech companies, though enforcement decisions might be different depending on the actors.

However, while some fines seem dissuasive and more proportionate towards SMEs, there hasn't been a fine imposed in the EU capable of **detering big tech companies** from abusing their users' data. For example, the biggest fine to date under the GDPR represented only 0.05% of Google's annual worldwide turnover. Therefore, much stronger enforcement is needed in the future against these companies to put a stop to these companies' unlawful data harvesting practices.

REPRESENTATION OF DATA SUBJECTS (ARTICLE 80(2) GDPR)

According to Article 80 of the GDPR, a body, organisation, or association may start an action on behalf of data subjects under certain conditions:

- [Article 80\(1\)](#) allows representative entities **under data subjects' mandate**, to exercise the rights of Articles 77-79 of the GDPR and the right to compensation and liability (Article 82 GDPR), where provided for by national law.
- [Article 80\(2\)](#) offers Member States the possibility to allow entities to exercise the rights of Articles 77-79 of the GDPR **without data subjects' mandate**. In this particular case, however, the right to compensation is excluded.

Article 80(2) limits the possibility for NGOs and consumer groups active in the field of data protection to bring complaints, including collective ones. By leaving it up to Member States to decide whether to allow groups to bring claims without data subjects' mandate, this provision created fragmentation on access to remedy. As a result, the enforcement of rights might not be the same across the EU depending on whether a Member State has put this avenue in place. We look forward to the conclusion of the negotiations of the Representative Action Directive, which should cover the GDPR, and the ePrivacy legislation, in order to improve access to remedy for users across the EU in case of data protection violation.¹⁵

We found the possibility of representative action without a mandate in the national adaptation laws of only **three Member States**: Belgium, France, and Denmark.¹⁶

To be more precise, France and Belgium did not technically implement Article 80(2), but they have amended their collective redress legislation in order to encompass claims against data protection violations.

This also does not mean that the possibility of bringing collective complaint without mandate does not exist in the other 25 Member States, as they might provide for this already in their legislation. This is the case for Germany, the Netherlands, and Spain, for example.

¹⁵ See Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC COM/2018/0184 final - 2018/089 (COD). Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0184>.

¹⁶ See "The collective private enforcement of data protection rights in the EU", A. Pato, 2019, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3303228; See "The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Rights", A. Pato in "National adaptations of the GDPR", K. McCullagh, O. Tambou and S. Bourton, 2019, available at <https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf>.

The lack of a harmonisation under the GDPR means that Member States rely on their own national laws instead of creating new avenues for remedy. This leads to sources of **misalignment with Article 80 of the GDPR as a whole**, especially regarding the right to bring a complaint.

Indeed, most Member States have more stringent conditions for right to bring a complaint than the one provided under the GDPR, as avenues for collective redress were generally created under general consumer laws. Therefore, in some countries, like Spain or Germany, collective action is only available to consumers, which limits the personal scope of the action. Moreover, conditions might be more stringent for associations or NGOs, with countries asking for a certain number of years of existence or a certain number of members, such as Germany, Belgium, and France. **These conditions are not mentioned in the GDPR and lead to further limitation of users' right to remedy.**

National laws might also not cover the full material scope of Article 80, limiting the claims possible, such as in Germany where the claims arising from the violation of the rights to information, to rectification, and erasure are not covered.

Finally, it should also be noted that, existing procedural tools might sometimes offer more advantages than the GDPR. For example, in some Member States, action for compensation without a previous mandate is possible.

PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC, OR HISTORICAL RESEARCH PURPOSES, OR STATISTICAL PURPOSES (ARTICLE 89 GDPR)

Article 89 provides for **safeguards and derogations** relating to the processing of personal data for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes. It does so in particular, for the processing of sensitive data (see Article 9(2)j.).

Pursuant to Article 89(1), Member States must put **safeguards** in place for when such processing occurs, to ensure data minimisation. One of the safeguards suggested is pseudonymisation.

According to Article 21(6) GDPR, where personal data are processed pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the **right to object** to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In addition to the “public interest” exception, Article 89(2) and (3) allow Member States to provide for **derogations** from the right to object, as well as rights referred to in Articles 15, 16, and 18 GDPR, in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. These derogations are subject to the conditions and safeguards referred to in Article 89(1).

If Member States allow it, personal data can be processed for public and non-public interests. However, “public interest” is not defined and the scope of this provision is consequently essentially left to the Member States.


Likewise, recital 159 of the GDPR explains that the processing of personal data for “scientific research purposes” should be interpreted in a broad manner, covering publicly and privately funded research. There is a risk therefore that marketing research could fall under this scope as well as encompassing companies that use personal data to further improve their services and develop new ones.¹⁷

And all this while data subjects are deprived of a number of important rights to be able to oversee such research (right to access, right to rectification, right to restriction of processing, and right to object).¹⁸

- **Sixteen Member States** chose not to provide for additional safeguards beyond the one provided under the GDPR for the processing for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes: Belgium, Bulgaria, Cyprus, Czech Republic, France, Greece, Hungary, Ireland, Italy, Lithuania, Malta, The Netherlands, Poland, Romania, Slovakia, and Spain.

This means that, even though the GDPR provides for appropriate safeguards to be put in place, these Member States did not expressly mention **what safeguards they implemented or if these even exist in their national legislation.**

- **Twelve Member States** added conditions or details for the processing of data for these purposes, including which safeguards they chose to implement, the majority being anonymisation or pseudonymisation:

| | |
|---|---|
|  <p>Austria</p> | <p>added <u>conditions</u>. Personal data may be processed for scientific research or statistical purposes if:</p> <ul style="list-style-type: none"> (a) It is publicly accessible; (b) the controller obtained the data through other investigations or for other purposes via permissible means; or (c) the data are pseudonymised for the controller and it cannot identify the data subjects via legally permitted means. <p>Personal data that do not fall into the above categories may only be processed for scientific research or statistical purposes:</p> <ul style="list-style-type: none"> (a) in accordance with specific statutory provisions; (b) with the consent of the data subject (s); or (c) with the authorisation of the Austrian DPA. <p>They also added <u>anonymisation requirement</u>: personal data must be anonymised as soon as the scientific research or statistical purposes no longer require identifiable data.</p> |
|---|---|

¹⁷ See “The Influence of Article 89 GDPR on the Use of Big Data Analytics for the Purpose of Scientific Research”, D. Koevoets, 2017, available at <http://arno.uvt.nl/show.cgi?fid=142885>.

¹⁸ See “The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks”, C. Staunton, S. Slokenberga, D. Mascalzoni, European Journal of Human Genetics, 2019, available at <https://doi.org/10.1038/s41431-019-0386-5>.



Croatia

specified that as a safeguard, personal data processed for statistical purposes must not allow identification of data subjects.



Denmark

added as a safeguard that the data subject is entitled to object to the processing of personal data relating to that person, unless the processing is necessary to perform a task in the public interest.



Estonia

specified that as a safeguard, personal data may be processed and transferred in a pseudonymised format or a format which provides equivalent level of protection.

If scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate. With regard to any personal data retained at the National Archives, the National Archives shall have the rights of the ethics committee.



Finland

specified that as a safeguard, the information is not disclosed or made available in a way that identifies a particular person unless the information is released for public statistics.



Germany

specified that, as a safeguard, special categories of personal data as referred to in Article 9(1) shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject.



Latvia

added a safeguard that if data are processed for archiving purposes in the public interest in order to create, collect, evaluate, preserve, and use national documentary heritage, a data subject shall exercise the rights specified in Articles 15 and 16 of the GDPR in accordance with the laws and regulations governing the area of archives.



Luxembourg

added multiple safeguards, including anonymisation or pseudonymisation.



Portugal

specified that, as a safeguard, the anonymisation or pseudonymisation of data shall be used. They added that consent

regarding the processing of data for scientific research purposes may cover several areas of research or be given only to certain specific fields or research projects, and in any case the ethical standards recognised by the scientific community should be respected.

 **Slovenia**

specified that as a safeguard, the user referred to in the preceding paragraph shall be transmitted in a pseudonymised form unless the pseudonymised data make it impossible to understand the purpose of the research or in which case the implementation of the research would be connected with disproportionate effort or costs.

 **Sweden**

added that personal data processed solely for research or statistical purposes may be used to take action on the data subject only if there are particular reasons for the vital interests of the data subject.

 **The UK**

restricted users' rights related to the processing of personal data for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes, including the right to object.

II. EVALUATING PROGRESS: MORE WORK IS NEEDED TO PROTECT USERS' RIGHTS AND CHANGE BUSINESS BEHAVIOUR

ROOM FOR IMPROVEMENT

Twelve months in, the GDPR has had mixed results. **On the one hand**, the awareness around data protection, users' rights, and avenues for remedy has increased. In 2015, before the adoption of the GDPR, only one third of the EU population was aware of the existence of data protection authorities.¹⁹ Now, more than half is aware which represents a considerable 20% increase in three years.²⁰ To assist in the awareness raising process, Access Now had developed a user guide to present the different rights under the GDPR, provide a model letter for exercising them, and give contact information for all data protection authorities.²¹

The number of complaints and data breaches notifications have also significantly increased over the last year. According to data published by the EU Commission, a total of 144,376 complaints were introduced across the EU between 25 May 2018 and 25 May 2019. Overall, all data protection authorities are reporting an increase in the number of complaints received post-GDPR. In France, the CNIL has received 30% more complaints compared to the previous year, which was already a record year.²² Similarly, in Belgium, the new data protection authority has received nearly double the number complaints than in 2017.²³ The same goes for the United Kingdom, the Netherlands, Italy, and nearly all authorities across the EU.²⁴

An increasingly large number of data breach notifications has been submitted across the last 12 months, suggesting that businesses and other organisations treat seriously the obligation imposed by Article 33 of the GDPR. Many DPAs have indicated a sharp increase in the number of data breach notifications when compared to the same period last year. According to data published by the EU Commission, a total of 89,271 data breach notifications have been submitted across the EU between 25 May 2018 and 25 May 2019.²⁵ This is not an indication that more breaches are happening now that the GDPR is in place, but that they are being reported more often. This change is positive for users, who have the opportunity to be better informed about how to protect their information that may have been accessed by an unauthorised party. Through the notification process, data processing entities have an incentive to create more robust systems and strengthen data security by developing updates and improving standards.

¹⁹ See "Hands off our data!", J.P. Albrecht, 2015. Edition Knauer Taschenbuch.

²⁰ See "The GDPR in numbers", EU Commission, 2019. Available at https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers.pdf.

²¹ See "A user guide to data protection in the European Union", Access Now, 2018. Available at https://www.accessnow.org/cms/assets/uploads/2018/07/GDPR-User-Guide_digital.pdf.

²² See "1 an de RGPD : une prise de conscience inédite", CNIL, 2019. Available at <https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite>.

²³ See "Le RGPD après six mois : bilan", Autorité de protections des données, 2018. Available at <https://www.autoriteprotectiondonnees.be/news/le-rgpd-apres-six-mois-bilan>.

²⁴ For reference, see the section "GDPR in numbers" of the bi-monthly newsletter GDPRToday. Available at <https://www.gdprtoday.org/>.

²⁵ See "The GDPR in numbers", EU Commission, 2019. Available at https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers.pdf.

On the other hand, we have highlighted in this report several issues with the implementation and enforcement of the GDPR, from risks of fragmentation to the slow resolution of complaints. This last issue can be attributed partly to the fact that the resources and number of staff for data protection authorities has largely remained the same in all Member States. This means that many authorities do not necessarily have the sufficient means to adequately respond to the growing number of requests and ensure that the data protection rights of EU data subjects are protected and enforced.

Worse still, a number of measures adopted in Member State adaptation laws seem to contradict the spirit of the GDPR. For instance, in November 2018, the Spanish Parliament passed a data protection law which contained a provision allowing political parties to use data subjects' personal information that had been obtained from web pages and other publicly accessible sources when conducting political activities during election campaigns.²⁶ The provision further authorised political parties to send citizens messages via social media and “equivalent media” without consent. Citizens could opt out if they did not wish their data to be processed. However, even if citizens did object to receiving political messages, they could still be profiled on the basis of their political opinions, philosophical beliefs, or other special categories of personal data particularly protected under the GDPR. This case raised serious concerns among the NGOs and representatives of the EU Parliament who saw in this provision several violations of the GDPR, including of the principles encompassed under Article 5 and the right to object. In May 2019, in a victory for users' rights, the Spanish Constitutional Court invalidated this provision, thus preventing a dangerous deviation from the GDPR in Spain.²⁷

THE ROLE OF DATA PROTECTION AUTHORITIES

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. Throughout this report we have raised the importance for Member States to respect 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.

The current lack of resources and the restructuring of most of these authorities to prepare for the GDPR can partly explain the slow enforcement of the law so far. We also note that a number of authorities, including the French CNIL, present themselves as partners to data processing entities and see their role as providing “guidance” and to “accompany” in their compliance exercise.²⁸ While we appreciate and acknowledge the value of the guidance and recommendations provided, DPAs' first responsibility under Article 51 of the GDPR is “monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing”. Priority must be given to users, their rights, and their complaints.

Addressing the elephant in the room, we must consider the unique role of the Irish Data Protection Commission (DPC). As a result of more than 70 years of economic transformation which encourages foreign investment, in particular from the US, Ireland has become the 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

²⁶ See Article 58 bis 1 of the Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, Spain. Available at http://noticias.juridicas.com/base_datos/Admin/lo5-1985.html.

²⁷ See “Nota Informativa 74/2019”, Tribunal Supremo de España, 2019. Available at https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_074/NOTA%20INFORMATIVA%20N%C2%BA%2074-2019.pdf.

²⁸ See “1 an de RGPD : une prise de conscience inédite”, CNIL, 2019. Available at <https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite>.

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 at the Irish level. Reports have revealed how tech executives pressured the Irish government to protect their beneficial tax arrangements. Now, data protection enforcement has also become a target for lobbying.²⁹ Many leading tech companies, with the exception of Amazon, Uber, and Netflix, have chosen Ireland as their main establishment under the GDPR, thus giving the Irish DPC a central role in enforcing the law for the (already many) complaints brought against these companies. For obvious reasons, the Irish DPC's willingness to make full use of its powers, including applying deterring 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 12 months in to the application of the law, and with many complaints filed, at the time of publication of this report, we are still waiting for the first decision on a complaint or investigation.

To protect EU data subjects' rights, the Irish DPC must now make use of all the powers and sanctioning mechanisms available under the GDPR. As tech companies seek to avoid falling under the jurisdiction of other data protection authorities, even if they process data of users across the EU, we must prevent forum shopping in the protection of personal data. In that context, the role of the EU Commission and of the European Data Protection Board when applying the cooperation and consistency mechanisms will be crucial.

THE RISK OF “BUSINESS AS USUAL”

Since May 2018, we have seen some encouraging signs to show that decisions driven by compliance with the GDPR have led not only to better protections for users, but also better customer service and growth in corporate revenue.³⁰ Innovating on data protection can lead to increased profit, and we hope that many more companies will adapt their business models to reflect this reality. For the time being, we unfortunately note that a large number of businesses and public entities are continuing with data practices that raise serious compliance concerns, not just with the GDPR but with the basic data protection principles that have been in place in the EU since 1995.

Companies are continuing to track users online, on websites, across platforms, and through their devices, without a valid legal basis, and without users' knowledge of such processing. In this context, the interaction between the GDPR and the current ePrivacy Directive is particularly relevant. With the entry into application of the GDPR, the definition of consent now also applies to the processing of data covered by the ePrivacy Directive.³¹ Entities can no longer hide behind the fragmented implementation of this ePrivacy Directive, which has led to the interpretation in some Member States that offering users an opt-out mechanism for cookies and trackers was an acceptable way to express consent. The GDPR requires an informed, explicit, affirmative action from the users which clarifies that pre-ticked boxes or opt-out systems are not a valid way to express consent. While we await for the completion of the ePrivacy reform, which should further clarify this

²⁹ See “How one country blocks the world on data privacy”, Nicholas Vinocur, 2019. Available at <https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123>.

³⁰ See “After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue”, Digiday UK, 2019. Available at <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/> and “Report: GDPR-Compliant Companies Experience Shorter Sales Delays”, D.Clark, 2019. Available at <https://www.law.com/therecorder/2019/02/06/report-gdpr-compliant-companies-experience-shorter-sales-delays/?sreturn=20190310123507>.

³¹ See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>.

reality, the EU Court of Justice is about to rule on the matter in the case C-673/17 *Planet 49*.³² The Advocate General in this case published its opinion in March 2019, indicating that, indeed, pre-ticked checkboxes do not constitute valid consent under the GDPR, the ePrivacy Directive, and the Directive EC/46/1995, which preceded the GDPR. This means that such practices have been contrary to EU law since 1995, even though they unfortunately continue to this day.

We further note that a number of companies are relying on specific designs to discourage users from exercising rights or forcing consent. A report by the Norwegian Consumer Council, *Deceived by Design*, highlighted the “dark patterns”, default settings, and other features and techniques used by companies to nudge users towards intrusive options.³³ The report analyses the practices of three companies and found that users were forced into privacy-intrusive default settings while privacy-friendly choices had been hidden away; that consent was provided on a “take-it-or-leave-it” approach; and that choice in design and architectures made users go through disproportionate efforts to set privacy-friendly options.

The novelty of the GDPR was not to introduce data protection obligations and rights, as most of these existed since 1995 in the EU; the real change came from the introduction of concepts such as accountability and data protection by design and by default. With these concepts, the long-term objective is to create a shift in the way data processors consider data protection, away from a mere compliance mindset. A year into the application of the GDPR, the data protection by design and by default mindset is far from becoming an industry standard, as most large tech companies and a majority of online actors are yet to abide by basic principles of the law. From lack of transparency to invalid consent, from large-scale tracking to deceiving practices, and more, there is plenty of evidence to show that it is high time to put an end to the “business as usual” attitude and enforce the law to make GDPR promises a reality.

“THE WHOLE WORLD IS WATCHING US”

While in this report we focused our analysis on the implementation and enforcement of the law, it is important to note that the GDPR has an impact globally. During the GDPR negotiations, former EU Justice Commissioner Viviane Reding noted that the “whole world is watching us reforming our data protection rules”.³⁴ There was a pressure to get the data protection reform right, not just for the impact it would have in the EU but also for the standard it could set for other countries. The adoption of the GDPR had global repercussions because of its extraterritorial scope and due to its domino effect. Professor Graham Greenleaf noted that since the adoption of the GDPR, the number of countries that have enacted data protection and privacy laws “has risen from 109 to 120, a 10% increase, with at least 30 more countries having official bills for such laws in various stages of progress”.³⁵ Countries such as Argentina or Japan have updated their data protection norms in the hope of maintaining or obtaining an adequacy status. Other countries like Brazil and Jamaica adopted their first data protection law, while countries like India, Tunisia, and the United States are

³² See Advocate General opinion in case C-673/19 *Planet 49*, 21 March 2019. Available at <http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9590369>.

³³ See “Deceived by Design”, Forbrukerradet, 2018. Available at <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

³⁴ See “Vice-President Reding’s intervention during Justice Council Press Conference, 6 June 2013”, EU Commission. Available at http://europa.eu/rapid/press-release_SPEECH-13-514_en.htm.

³⁵ See “Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey”, G. Greenleaf, 2017. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035.

immersed in considerably advanced debates for the passage of a law, or sometimes several such laws.³⁶

Much like what happened with the GDPR, these debates are taking place under intense political pressure and corporate lobbying. Companies whose business model involves harvesting personal data do not submit easily to the idea of governments reining in these practices for the benefit of users' rights. Since the GDPR has contributed to igniting a global race for data protection, many companies would like to see the GDPR fail.³⁷ In this context, no buzzword and taglines will be spared to undermine the law: the GDPR has been accused of helping big tech and simultaneously of taking aim at big tech; of killing SMEs and of being bad for business; of being bad for Europe; of being a bad idea altogether; of being a trap; of being evil; of being bureaucratic; and of being the end of the internet.

The GDPR is far from perfect and we are seeing mixed results in the first 12 months of enforcement. Enforcement, awareness-raising, and change of behaviour are understandably taking time as authorities needed to provide guidance and re-organise their own functioning. But it is now time to act as the world continues watching us. We should not underestimate the importance of getting the enforcement of the GDPR right for businesses and users in the EU, and for the impact beyond the EU borders.

³⁶ To assist governments around the world being inspired to upgrade or develop data protection legislation, Access Now has developed a guide based on our experience with the GDPR. See "Creating a data protection framework: A do's and don'ts guide for lawmakers", Access Now, 2018. Available at <https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf>.

³⁷ See "Revealed: Facebook's global lobbying against data privacy laws", The Guardian. Available at <https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment>.

III. RECOMMENDATIONS: MOVING THE GDPR APPLICATION AND ENFORCEMENT FORWARD

To address some of the issues and challenges detailed in this report, Access Now has prepared recommendations directed at the EU Commission, the Member States, 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 THE MEMBER STATES

-
- Member States must provide their national data protection authorities with appropriate **financial and human resources** so that they can conduct their monitoring, investigation, and supervision tasks adequately.
-
- Member States must ensure the **independence** of their national data protection authorities, both in terms of budget and powers. National authorities' structure, functioning, and priorities shall be defined in a transparent manner. Reforms shall be conducted to ensure that executive bodies, including the heads of states and governments, shall not interfere or be involved in the nomination, organisation, and functioning of data protection authorities.
-
- Member States must ensure that their **national adaptation law respects the spirit, essence, and content of the GDPR** to ensure harmonisation and a consistent high level of data protection across the EU.
-
- Member States must **move forward the negotiations of the Representative Action Directive** in Council. The scope of this legislation should cover the GDPR and the ePrivacy legislation in order to improve access to remedy for users across the EU in case of data protection and privacy violation.
-

2. RECOMMENDATIONS TO THE EU COMMISSION

-
- The EU Commission must **guarantee a harmonised implementation of the GDPR** across the 28 Member States. In this task the EU Commission must ensure that national adaptation laws are not departing from the GDPR and intervene in cases where the Member States impose conditions or reduce the scope of application of users' rights.
-
- The EU Commission must **launch infringement procedures** against Member States when violations of the GDPR are reported due to incorrect implementation of the law.
-

- The EU Commission must call on **Portugal, Slovenia, and Greece to adopt a national law** implementing the GDPR and provide for a deadline after which the EU Commission will start infringement proceedings.
-

3. RECOMMENDATIONS TO THE NATIONAL DATA PROTECTION

AUTHORITIES

- DPAs must **prioritise the processing of users' complaints** and put in place processes to provide more transparency around enforcement actions

 - DPAs should **conduct investigations into deceiving practices**, such as forced consent through design patterns or vague policies.

 - DPAs must **make full use of the enforcement mechanisms** by imposing deterrent fines complemented with orders prohibiting unlawful practices to continue.

 - DPAs should **continue to provide guidance** on how to implement the GDPR for businesses, public entities, and users.
-

4. RECOMMENDATIONS TO THE EUROPEAN DATA PROTECTION BOARD

- The European Data Protection Board **must prevent forum shopping of representation** and ensure harmonisation in the application of the GDPR.

 - The European Data Protection Board **must increase transparency of its meetings** by publishing minutes.

 - The European Data Protection Board **must ensure consistency** in the resolution of cross-border cases. To that end, the EDPB should **develop guidelines for cooperation** between data protection authorities that must require transparent processes.
-

CONCLUSION

In the movie *Democracy: Im Rausch der Daten*, which documents parts of the negotiation process of the GDPR, Joe McNamee, former director of the NGO European Digital Rights, explained how Jan Philipp Albrecht, the EU Parliament Rapporteur for the law, had to accomplish what seemed to be an unachievable task: concluding an agreement on a text that would be acceptable for all political parties, Member States, and stakeholders.³⁸

The GDPR was one of the most lobbied pieces of legislation in the EU, and nearly 4,000 amendments were tabled during the negotiations in Parliament and debates in the Council of the EU, which lasted nearly three years. Yet Albrecht delivered on his impossible task. The final text of the law was adopted by an overwhelming majority of the EU Parliament, with support from all political sides. On the date of its adoption, 25 May 2016, no one was fully satisfied with law, perhaps not even the Rapporteur, but the result was still positive and brought promise for strengthening users' rights across the EU, under legislation fit for the digital age.

Much like its Rapporteur, the GDPR faced an impossible “task” for its first year of application: deliver on all its promises and make modern data protection a reality across the EU. After a two-year implementation period, which should have allowed everyone from data protection authorities to data controllers and processors to get ready (something rare for a Regulation, which is usually directly applicable from the day of entry into force), the GDPR was supposed to bring benefits from day one. It would be easy to see the mixed results we describe in this report as indicative of failure, or to view the GDPR as a boon to big tech over SMEs. That would ignore the reality of both the digital economy and the rule of law. Implementing the long-term changes and realising the promises of the GDPR will take time. We cannot expect to change in 12 months practices and attitudes that have been in place for years.

Evaluating the success or failure of the GDPR will also take time. We are confident that despite the challenges faced in this first year, the promises of the GDPR will be delivered. We are encouraged by the growth in awareness of data protection, by the choices that some companies are making for a data protection and privacy business model, and by the first few enforcement cases. With long-term investment and commitment from the EU Commission, the Member States, DPAs, the EDPB, and the help of civil society, the GDPR has the potential to be one of the EU's greatest successes in the protection of fundamental rights.

³⁸ See “Democracy: Im Rausch der Daten”, David Bernet, 2015. More information available at <https://www.imdb.com/title/tt5053042/>.

ANNEX - GDPR NATIONAL ADAPTATION LAWS

| | |
|---|--|
|  Austria | → <u>Datenschutz-Anpassungsgesetz 2018</u> |
|  Belgium | → <u>Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel / Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens</u> |
|  Bulgaria | → <u>Закон за защита на личните данни</u> |
|  Croatia | → <u>zakon o provedbi opće uredbe o zaštiti podataka</u> |
|  Cyprus | → <u>Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (125(I)/2018)</u> |
|  Czech Republic | → <u>Návrh zákon o zpracování osobních údajů</u> |
|  Denmark | → <u>Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)</u> |
|  Estonia | → <u>Isikuandmete kaitse seadus</u> |
|  Finland | → <u>Tietosuojalaki (1050/2018)</u> |
|  France | → <u>LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles</u> |
|  Germany | → <u>Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs und -Umsetzungsgesetz)</u> |
|  Greece | → Draft law - <u>Νόμος για την Προστασία Δεδομένων Προσωπικού Φαρακτόρα</u> |
|  Hungary | → <u>Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló</u> |
|  Ireland | → <u>Data Protection Act 2018</u> |
|  Italy | → <u>DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”</u> |

| | |
|--|---|
|  Latvia | → <u>Fizisko personu datu apstrādes likums</u> |
|  Lithuania | → <u>Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo</u> |
|  Luxembourg | → <u>Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)</u> → <u>Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale</u> |
|  Malta | → <u>Data Protection Act, Cap. 586 (May 28, 2018)</u> |
|  The Netherlands | → <u>Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming)</u> |
|  Poland | → <u>Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych</u> |
|  Portugal | → Draft law - <u>Proposta de Lei n.º 120/XIII</u> |
|  Romania | → <u>LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)</u> |
|  Slovakia | → <u>Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (18/2018)</u> |
|  Slovenia | → Draft law - <u>predlog Zakona o varstvu osebnih podatkov –predlog za obravnavo –nujni postopek–NOVO GRADIVO ŠT. 2</u> |
|  Spain | → <u>Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales</u> |
|  Sweden | → <u>Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning</u> |
|  The UK | → <u>Data Protection Act of 2018</u> |

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, and convenings such as RightsCon, we fight for human rights in the digital age.

<https://www.accessnow.org>

