January 31st, 2020

Access Now's response to questions shared on the multi-stakeholder expert group to support the application of Regulation (EU) 2016/679

QUESTIONS TO INFORM THE PREPARATION OF THE EVALUATION REPORT OF MAY 2020 ON THE APPLICATION OF GDPR

Access Now welcomes the opportunity to provide feedback to the questions outlined below in writing. These answers reiterate and complete the oral comments provided at the multi-stakeholder group meetings on 18 September 2018 and 5 March 2019 and the first round of written comments submitted in November 2018 and April 2019.

General comments

Please explain what were the main issues your stakeholders experienced, or you have observed, on the application of GDPR.

As we approach the two year anniversary of the entry into application of the law, we have witnessed the first positive impacts of the GDPR. People living in the EU have been exercising their rights and an increasing number of data breaches have been reported to authorities, allowing those authorities to respond to mitigate risks for users. Data protection authorities have also timidly started enforcing the law, but for the GDPR to reach its full potential, we need to see stronger, more coordinated enforcement.

Regarding improved business practices, we have seen some encouraging news showing how compliance decisions driven by the GDPR have led to not only more privacy protections for users, but also growth in revenue and better customer service.[1] Data protection innovation can lead to profit and we hope that many more companies will adapt their business-model to this reality. For the time being, we still note that a large number of businesses - and public entities - are continuing with data practices that raise serious compliance concerns with even the most basic data protection principles in place in the EU since 1995. To put an end to this "business as usual" attitude and make GDPR a reality, data protection authorities must be more (pro)active in enforcing the law. To help with this process, member states must increase the funding and staffing of their data protection authorities. The 2019 report of the European Data Protection Board shows that in most EU states, financial and human

[1] See for instance: https://www.law.com/therecorder/2019/02/06/report-gdpr-compliant-companies-experience-shorter-sales-delays/?slreturn=20200031134834 and https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/

resources are insufficient.[2] As a result, authorities might not be able to properly and effectively perform their tasks, in particular a number of complaints coming in continue to grow.

Impact of the GDPR on the exercise of the rights

Based on official numbers communicated by the EU Commission and Data Protection Authorities, we note an increase in the number of users' exercising their data protection rights across the EU since the GDPR became effective in May 2018.[3]

However, many companies have yet to adapt their behaviour to implement data protection by design and by default requirements. Many companies are continuing to track users online, across websites, platforms, and through their devices, often 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. Entities can no longer hide behind the fragmented implementation of this 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. We also note that Member States are lagging behind in ensuring implementation of these obligations. According to a presentation given by the EU Commission in Council in January, only 3 out of, now, 27 EU countries have properly adapted their legislation transposing the ePrivacy Directive to comply with the GDPR.

While we await the completion of the ePrivacy reform, which should further clarify how rules complement each other, the EU Court of Justice ruled on a related matter in the case C-673/17 *Planet 49.* Following the opinion of the Advocate General in this case, the Court ruled that 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 privacy-invasive behaviors that users in the EU continue to experience have been contrary to EU law since 1995. Member States and regulatory bodies must step up the enforcement of these norms.

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.[4] 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

---

[2] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

[3] https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf

[4] https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

"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. Nearly two years 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.

Complaints and legal actions
Use of representative actions under Article 80 GDPR
Experience with Data Protection Authorities (DPAs), the one-stop-shop mechanism (OSS) and the consistency mechanism (opinions under Article 64 GDPR)

A large number of Access Now's partners, fellow members of the EDRi network have filed complaints under the GDPR all across the EU. These complaints will help bring GDPR protections into reality for users and may contribute to the development of guidance and jurisprudence ensuring harmonised implementation of the law across the EU.

From these experiences, we note that procedural hurdles remain in place for NGOs to bring complaints, in particular when cross-border in nature. This is partly due to the fact that many member states have not made use of Article 80.2 of the GDPR which would allow groups to bring forward collective complaints without having to be directly mandated by users. This means that access to remedy and the enforcement of rights might be unequal across the EU depending on whether or not member states have 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.

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

The ongoing lack of resources and the restructuring of most of these authorities when preparing for the GDPR can partly explain the slow enforcement of the law so far. We also note that a number of authorities, including the Spanish AEDP, present themselves

as partners to data processing entities and see their role as providing "guidance" to "accompany" their compliance exercise. This has for instance led the AEDP to publish joint guidelines on the use of cookies with the ad and digital marketing firm IAB Spain. These guidelines not only contradicted the guidance provided by most EU data protection authorities, thus causing confusion for online actors on how to comply with the law but also greatly undermine the trust in the authority as an independent body considering the economic interest of IAB in these guidelines. We note that 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". We therefore call on the authorities to give priority to users, their rights, and their complaints.

Finally, 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 a safe haven for tech giants. In the 80's, tech companies such as Apple, Microsoft, Dell, and Intel established manufacturing plants in the country, taking advantage of significant tax cuts and establishing themselves as major investors and employers. As the years passed and as more companies established their European base in Ireland, tech giants have arguably gained an unprecedented level of influence in policy debates in Ireland. Reports have revealed how tech executives pressured the Irish government to protect their beneficial tax arrangements.[5] Now, data protection enforcement has also become a target for lobbying.[6] Many leading tech companies, such as Facebook, Google, Apple and Microsoft, 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. With pressures coming from tech giants and the own Irish government, the Irish DPC's ability to make full use of its powers, including imposing fines against these large companies for GDPR violations, remains questionable. The DPC has opened several investigations since the entry into application of the GDPR, but 20 months in to the application of the law, and with many complaints filed, at the time of filing of these comments we are still waiting for the first decision on a complaint or investigation.

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 EU Commission and the European Data Protection Board have a central role in ensuring the proposer functioning of the cooperation and consistency mechanisms. To protect EU data subjects' rights, we do not see a need to reform rules designed under the GDPR but to instead ensure that all the options provided by the law, including the use of emergency procedures, are utilised.

Have you experienced or observed any problems with the national legislation implementing the GDPR (e.g. divergences with the letter of GDPR, additional conditions, gold plating, *fragmentation*, etc.)?

[5] https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123
[6] https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123

In May 2019, Access Now published a report in which we highlighted several issues with the implementation and enforcement of the GDPR, from risks of fragmentation to the slow resolution of complaints.[7]

Several member states have widely used the exception available under the law to create specific national rules on a number of aspects. In the best case scenario of this bad situation, the use of some of these exceptions is creating fragmentation in the implementation of the law. In the worst case, they contradict the spirit, objective and, text of the law. We call on the EU Commission to intervene in countries where member states have implemented a national law that undermine the core 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. 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. The Spanish law, however, still includes problematic provisions that either contradict or go beyond the rules established under the GDPR. For instance, this is the case for Article 94 of the LOPD on a "right to be forgotten" which requires the deletion of content from social media platforms.[8]

The Commission must make full use of its powers as Guardian of the Treaties and firmly address these issues. Failure to do so could lead to gross misunderstanding and misrepresentation of the GDPR thus undermining the law and the benefits it brings to people.

GDPR and new technologies

a. **How do you assess the overall impact of GDPR on the approach of organisations you represent to innovation?**
b. **How do you assess the impact of GDPR on the development of new technologies, such as artificial intelligence, blockchain, internet of things, etc.? Please provide concrete details.**
c. **Do you think that GDPR provides sufficient protection for the trustworthy development of new technologies such as artificial intelligence?**

[7] https://www.accessnow.org/cms/assets/uploads/2019/07/One-Year-Under-GDPR-report.pdf
[8] https://www.boe.es/eli/es/lo/2018/12/05/3/con

d. **In respect of artificial intelligence, what could be the potential gaps with respect to the protection of individuals' personal data for which further policy action may be necessary?**

The General Data Protection Regulation is a technology-neutral law that applies to the processing of data offline and online, including when using technologies like artificial intelligence, blockchain, or the internet of things. Thanks to obligations under the GDPR and other norms, technologies must and can be developed in a way that they respect data protection, privacy, and security by default.

The EU Ethics Guidelines for Trustworthy Artificial Intelligence developed by the High-Level Expert Group recall that for the development of AI systems: "besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data". The accompanying document makes ample references to the GDPR and the need to ensure compliance with it. Beyond the GDPR, it would be helpful to develop requirements to ensure that AI developers take into account and mitigate the impact that their systems can have on users' rights based on data not provided by the users itself and either generated or brought by an external source.

Adequacy decisions and other transfer tools

a. **Do the organisations you represent rely on adequacy decisions for their international transfers and, if so, which are the main "destination" countries/territories to which data is sent using this transfer mechanism?**
b. **What is you experience with using adequacy decisions as a mechanism for transferring data? Did you encounter any particular question or concern when relying on any of the adequacy decisions adopted under the 1995 Directive (with the exception of the EU-US adequacy decision which is covered by a separate, and annual, review process)?**
c. **Do you have any information on the developments of the data protection system of any of the countries/territories subject to a Commission adequacy decision under the 1995 Directive that you would consider relevant for the Commission's evaluation?**
d. **In your view, should any other third country be considered by the Commission in view of a possible adequacy decision?**
e. **What other transfer mechanisms from the GDPR toolbox should be developed as a matter of priority?**

Users benefit from a free, open, and secure internet that is enabled by legal certainty for stakeholders to operate. Robust data transfer frameworks which ensure a high level of data protection in the free flow of data are key to deliver these benefits for all actors.

Access Now regularly analyses data transfer arrangements under EU law. In particular, Access Now has provided detailed analysis and recommendations to the EU Commission on how to improve the EU-US Privacy Shield since negotiations began in 2016. At the invitation of the EU Commission, we send detailed comments on the

functioning of the EU-U.S. Privacy Shield every year during the annual review process.[9] The Privacy Shield continues to be inadequate to protect fundamental rights. To protect users' privacy and data protection when personal data is transferred, we have called on the EU and the U.S. to conduct comprehensive and necessary reforms. These include surveillance reforms on both sides of the Atlantic and the enactment of a binding data protection framework in the U.S. and access to remedy for non-U.S. persons, including data subjects in the EU. In the absence of these important reforms, the Privacy Shield has manifestly failed to meet the standards set by EU law from inception to today. While we await for several court decisions from the CJEU that may set the future of this arrangement, we reiterate our call to the EU Commission to suspend this ill-suited framework.

Going forward, Access Now will also contribute to the review of the EU-Japan adequacy decision. We further plan to contribute to debates surrounding the potential renewal of the adequacy status to Uruguay and Argentina and to the opening of new adequacy decision negotiations with latin american countries. Finally, at the time of this submission, the United Kingdom is set to leave the European Union at midnight on January 31st. The EU and the United Kingdom have clearly expressed their willingness to finalise an adequacy decision by the end of the transition period set by the withdrawal agreement. As this period is currently set to conclude on December 31, 2020, these would potentially be the fastest negotiations for an adequacy decision. We note that there is no obligation for the EU to finalise negotiations by then and that this date is merely a wish expressed by parties. To get to that point, the UK will have to undergo a significant amount of reform to ensure that users' rights are safeguarded. It will also have to end blatant violations of EU laws such as the copying of databases.[10] While the UK currently has the obligation to apply the GDPR, it will be crucial to ensure that the country continues to apply high standards for data protection going forward. In addition, as established by EU jurisprudence, the UK will have to guarantee EU data subjects' with a right to remedy and it will have to ensure public authorities, including law enforcement authorities' processing of data is necessary and proportionate. This latter point suggests that the UK will need to reform most of its surveillance laws, many of which include measures that have been ruled disproportionate by the European Court of Human Rights in Strasbourg. Access Now will closely monitor and actively contribute to the EU-UK adequacy negotiations.

Closing comments

We appreciate the opportunity to submit comments to inform the preparation of the first evaluation report on the application of the GDPR to be published in May 2020. We hope that this process contributes to highlight the benefits brought by the GDPR and provide recommendations to improve its implementation.

---

[9] https://www.accessnow.org/cms/assets/uploads/2019/09/Access-Now-Submission-Privacy-Shield-Review-Questionnaire-Third-review-Final.pdf

[10] See for example: https://www.theguardian.com/world/2020/jan/09/uk-accused-of-behaving-like-cowboys-over-eu-database-copying and https://www.theguardian.com/uk-news/2020/jan/14/revealed-uk-concealed-failure-to-alert-eu-over-75000-criminal-convictions

During the negotiations of this legislation in Brussels, lawmakers have been faced with an unprecedented amount of lobbying, mostly trying to undermine the GDPR. Since its adoption, the law is seen worldwide as one of the major successes of the EU and one of the most protective framework for users. But the lobby to undermine it has not stopped. As the first review process is happening, many are using this opportunity to seek a reform of this law, and with it, to remove many of the provisions that safeguards users' rights. While it is true that the law has yet to deliver many of its benefits, it would be ill-advised for the EU to reform this law before it has been properly implemented and enforced.

The GDPR is far from perfect and we are seeing mixed results in the first 20 months of application. Enforcement, awareness-raising, and change of behaviour are understandably taking time as authorities needed to provide guidance and re-organise their own functioning. It is now time to act and enforce the law as the world continues watching us and the GDPR serves a global standard-setter for data protection. We should not underestimate the importance of getting the enforcement of the GDPR right for businesses and users in the EU, and for the impact beyond the EU borders.

We remain available for any questions you may have.

For more information, please contact
Estelle Massé, Global Data Protection Lead (estelle@accessnow.org)