April 2019

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

INFORMATION ON THE APPLICATION OF GDPR

Introduction

Access Now welcomes the opportunity to provide feedback to the questions outlined below in writing. These answers 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.

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

Nearly a year after the entry into application of the law, we have witnessed the first positive impacts of the GDPR. People living in the EU have been using their rights to access data, erasure, withdraw consent; a large number of complaints have been filed in front of the authorities and the data protection authorities have started enforcing the law by applying the first fines. But for the GDPR to reach its full potential, we need to move from the implementation to the enforcement stage.

On the side of business, we have seen some encouraging news showing how compliance decision driven by the GDPR has led to not only more privacy protections for users, but also growth in revenue and better customer service. 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 unfortunately note a large number of businesses - and public entities - are continuing with data practices that raise serious compliance concerns with even the most basis 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, 2019 must be the year of enforcement. For this, member states must increase the funding and staffing of their data protection authorities. The latest report of the European Data Protection Board shows that in some states, financial and human resources are significantly insufficient. 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.

Compliance with the GDPR is not only a matter for businesses and public entities. As an NGO with operations in the European Union, our organisation is required to comply with the GDPR. Processing personal data impacts fundamental rights, but is often necessary to enable us to achieve our mission of defending and extending the digital

rights of users at risk around the world. After several years of effort to uphold the rights and principles behind the GDPR, we are glad to report that our data processing activities are limited.

Since 2011, we worked for the strengthening of the GDPR during the legislative debates, advocated for its adoption, we contribute to its implementation and we are raising awareness on its value and benefits for users. This does not mean however that we consider compliance to be an easy task for data controllers and processors around the world. Compliance with new standards such as data protection by design and by default can take some time as well as the assessments of all internal and external data processing practices to evaluate practices and if need be, modify them. Guidance from the Data Protection Authorities on how to implement these new principles can facilitate compliance and we welcome their recent publication of the draft guidelines on the scope.

What is proven to be one of the most challenging issues for compliance is the attitude of a few member states towards the GDPR. Despite the two year period for the implementation of the law, three member states still have to adopt a national legislation adapting the law. In addition, 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. We particularly urge the Commission to take action against Romania, where the government is abusing the GDPR to seek journalists to reveal their sources, and against Spain, where the legislators adopted a wide exception from the GDPR to allow for the use of data by political parties which could lead to the profiling of people on the basis of their political views. 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.

2. **Impact of the GDPR on the exercise of the rights**
    a. **How have the information obligations (in Articles 12 to 14) been implemented? Has there been a change of practices in this respect?**
    b. **Is there an increase of requests (where possible provide estimates);**
        i. **to access data?**
        ii. **rectification?**
        iii. **erasure?**
        iv. **for meaningful explanation and human intervention in automated decision making?**
    c. **Are there requests on data portability?**
    d. **On which rights do these requests mostly relate to?**
    e. **Are there any difficulties in the application of the rights (by controllers, by DPAs), including for meeting the deadlines for responding to the requests?**
    f. **What percentage of the requests was manifestly unfounded or excessive? Please describe why these requests were unfounded or excessive.**

Since May 2018, Access Now has received a small number of requests for access, information, and erasure. We noticed a slight increase in these requests for this specific time period compared to the previous year. We have not received any request for portability or for explanation related to the use of automated decision making as we do not use such data processing techniques.

Through our work monitoring the implementation of the GDPR, we found that most businesses and several public entities still have a long way to go in guaranteeing users' the exercise of their rights under the GDPR. A number of companies, including through our discussions in the expert group, choose the highlight the minority of cases related to blatantly abusive requests. Cases of abusive requests will unfortunately exist, however the GDPR provides the means to deal with such scenarios. While a few companies chose to focus communications on these isolated abusive cases, users still face important hurdles to benefit from their rights. First, it is not always clear information as to where users can place their requests for access, erasure, and more. Entities must do more to clearly and proactively communicate to users the email address or platform through which they can exercise their rights. Then, entities must respect the time frame set under the GDPR to respond to these requests. Finally, data protection authorities should provide more guidance on how entities may require users identification. Currently, users may be requested to go through time consuming and counter-productive processes that may require to provide more personal data to an entity in order to exercise rights.

To assist users in the exercise of their rights, a number of NGOs have launched practical tools. Thanks to the Dutch NGO Bits of Freedom, through my Data Done Right, users can submit access, correction, deletion, and transfer requests. The tool also helps users keep track of their requests and compares their results with others who have made similar requests.

3. **Impact of Article 7(4) regarding the conditions for valid consent on your business model/consumers:**
    a. **Are there any issues with the use of consent as legal basis for specific processing operations? (e.g. complaints received) When requesting consent, how did individuals respond?**
    b. **Have you switched the legal ground for processing from consent to another legal ground?**
    c. **How are businesses addressing the issue of tied consent? How are they distinguishing between contract as legal basis and consent?**

After 25 May 2018, we have witnessed the wave of emails requesting users consent, updated cookie banners and reform of terms of services. These actions showed that a large number of data processors and controllers undertook a spring cleaning and looked into their data practices. While this spring cleaning could have been an opportunity to demonstrate greater awareness for data protection, the changes or communications put forward do not always leave up to the level required by the GDPR.

Many companies continue to track users online and through their devices without valid consent. 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 ePrivacy Directive which led to the interpretation in some member states that offering users an opt-out mechanism was an acceptable way to express consent. The GDPR requires an 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 the completion of the ePrivacy reform which should further clarify this reality, the EU Court of Justice is about to rule on the matter in the case C-673/17 *Planet 49.* The Advocate General in this case has published it opinion in March 2019 in which he indicates that, indeed, pre-ticked checkboxes do not constitute valid consent under the GDPR, the ePrivacy Directive but also under the Directive EC/46/1995 which preceded the GDPR. This means that such practices are contrary to EU law since 1995, even though they unfortunately continue nowadays.

Finally, we note that a number of companies are relying on specific designs to discourage users from exercising rights or force consent. A report by the Norwegian Consumer Council, Deceived by Design, highlighted the "dark patterns", default settings, features and techniques used by companies to nudge users towards intrusive options. The report analyses the practices of three companies and found that in users where 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 choice in design and architectures made users go through disproportionate efforts to set privacy friendly options.

4. **Complaints and legal actions**
    a. **Are there any complaints to the DPA against your organisation(s)?**
    b. **Are there any court actions against your organisation(s)?**
    c. **Are there any court actions against decisions, or absence of decisions, of DPAs?**
    d. **In all above cases, please explain what is the matter of the complaint or court action and for which types of infringements of GDPR?**

None.

5. **Use of representative actions under Article 80 GDPR**
    a. **As an organisation representing civil society, have you filed representative actions in any Member State?**
    b. **What types of representative actions (complaint to DPA or to court, claim for compensation)? In which country/ies?**
    c. **Against whom and for which types of infringements of GDPR?**

While Access Now did not file any complaints, we have been providing support and following the activities of fellow members of the EDRi network. On 25 May 2018, *noyb* - the European Center for Digital Rights - and La Quadrature du Net were among the first NGOs to file complaints at several data protection authorities across the EU, mostly around the issue of consent. Additional complaints on the right to access have since been filed by *noyb.* In November 2018, Privacy International filed complaints with three data protection authorities against data brokers and credit reference agencies in relation to profiling. In December and January 2018, Open Rights Group, Panoptykon Foundation and their partners filed complaints related to the functioning of online behavioural advertising ecosystem.

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.

Finally, we would like to highlight the procedural hurdles that 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 a 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.

6. **Experience with Data Protection Authorities (DPAs) and the one-stop-shop mechanism (OSS)**
    a. **Are there any difficulty experienced in the dealings with DPAs (by individuals/businesses)?**
    b. **Are there difficulties in obtaining advice or guidance material by the DPAs?**
    c. **Are DPAs following up on each complaint submitted, and in a timely manner?**
    d. **How many of your business members have declared a main establishment to a DPA and benefit from a Lead Authority? Have they experienced difficulties with the functioning of the OSS?**
    e. **Do you have experience with the designation of representatives of controllers or processors not established in the EU?**
    f. **Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines? (please explain)**

With the EDRi Network, our organisation works with partners to track the number of GDPR complaints and cases brought since May 2018. Through our project called the GDPRToday, we provide bimonthly information to data protection experts, data protection officers, lawmakers and authorities on the concrete implementation of the GDPR. So far, the numbers show a great interest from users to use the redress mechanisms available under the GDPR. While a number of cross-border cases and complaints have been filed, we are yet to fully learn from our partners on the experience with the one-stop-shop from the perspective of the individuals and NGOs as plaintiffs.
In general, guidance from DPAs on the functioning of the EDPB and the new one-stop-shop mechanism would be welcomed as this new system has yet to be fully tested.

7. **Designation of data protection officers (DPO)**
    a. **Did your organisation designate a mandatory DPO pursuant to Article 37(1) GDPR?**
    b. **Did your organisation designate a mandatory DPO pursuant to national law implementing Article 37(4) GDPR? Please specify which national law and for which situations.**

c. **Did your organisation designate a DPO on your own initiative, without being required to do so by the GDPR or by national law?**
d. **Did associations or other bodies representing categories of controllers or processors designate data protection officers?**
e. **What is the experience of the organisations you represent with the performance of DPOs?**

Our organisation has established a small internal team dedicated to tracking internal and external policies, responding to users' requests and monitoring compliance.

8. **Controller/processor relationship**

a. **What is the experience of your members on the adaptation of current contracts?**
b. **Is there a need for the adoption of standard contractual clauses under Article 28(7) GDPR? Explain what are the main reasons.**
c. **If standard contractual clauses were to be prepared, what elements and specifications should be included? (e.g. auditing, liability allocation, duty of cooperation, indemnification)?**
d. **Do you have suggestions in terms of how to ensure the "user-friendliness" of such standard contractual clauses?**
e. **In case you have drafting suggestions for specific clauses, please share.**

/

9. **Adaptation/further development of Standard Contractual Clauses (SCCs)**
    a. **What are your practical experiences with the existing SCCs: Do they serve the purpose? If not, where do you see room for improvements? Have you encountered any problems in using the existing SCCs?**
    b. **Do you see a need to adapt the existing SCCs, generally and/or in the light of the GDPR? (e.g. different structure/design? additional safeguards?; combination with Art. 28 standard clauses for processors?)**
    c. **Do specific clauses require further clarification (e.g. auditing, liability allocation, duty of cooperation, indemnification)?**
    d. **Is there a need to adapt the SCCs in light of the Schrems II court case (concerning access by third country authorities), e.g. with respect to monitoring/reporting obligations on the data importer/exporter? Do you have suggestions on ways and means to strengthen the possible control by the data exporter vis-à-vis the data importer and the measures to enforce such control (e.g. not only suspending the transfer of data but actually recalling the data already transferred?) Do you have any other suggestions on how to further strengthen data protection safeguards and control mechanisms (including by the DPAs) with regard to government access?**

e. **Is there a need to develop new SCCs, e.g. for the processor/sub-processor relationship, joint-controllership, processor-to-controller relationship or specific processing operations?**
f. **Do you have suggestions in terms of how to enhance the "user-friendliness" of SCCs?**
g. **In case you have drafting suggestions for specific clauses, please share.**

Note: *We consulted Max Schrems, chairman of noyb, on the general matter of SCCs and some of his feedback was included in our answer. The full questionnaire was however not shared with him.*

A few aspects of SCCs have worked relatively well, such as the certainty provided to the data controller and the relationship with DPAs, even if the issuance of the SCCs can sometimes be lengthy.

We do however see a need and opportunity to adapt the SCCs to the GDPR to correct issues with the format and content of the current forms (typos, erratas) and to reflect some of the new requirements and rights under the GDPR, including data security, data breach and reporting obligations. A reference to the new accountability principle would for instance be welcome to encourage entities to keep records of their decisions and actions. Additionally, data protection authorities should ensure greater scrutiny and increased control of the implementation of SCCs, including through proactive investigations and checks.

Further changes may be required in light of the upcoming ruling on the *Schrems II* case. Clarifications could be provided by making clear that there is a *duty* of the relevant data protection authority to prohibit transfers if a third country government is violating fundamental rights. In addition, recital 11 of the Commission Decision on SCCs from 2004 should be updated to reflect the changes that were brought to Article 4 to clarify that data protection authorities can indeed make full use of their powers to suspend transfers in case of fundamental rights violations. Finally, for increased transparency for the users and in line information rights under the GDPR, SCCs should be made available publicly and not just provided to the data subject on request.
Both for the upgrade in light of the GDPR and the implementation of the upcoming ruling, guidance from the EDPB will be crucial.

10. **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, etc.)?**

We have provided an answer to this question in the first question on general comments.

Conclusion

Access Now appreciates the opportunity to provide feedback to the EU Commission on the above questions related to the implementation of the GDPR.

Our organisation will continue to monitor the concrete impact of the law under the GDPRToday, together with a coalition of NGOs from the EDRi network. Finally, we will

continue our awareness efforts to promote the rights available under the GDPR to individuals in the European Union.

We remain available for any questions you may have.

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