

Re: The General Data Protection Regulation (GDPR) review by the European Commission

Dear Executive Vice-President Jourová,
Dear Commissioner Reynders,

European Digital Rights (EDRi) is an umbrella organisation with 44 NGO members with representation in 19 countries that promotes and defends fundamental rights in the digital environment.

For the second anniversary of the GDPR's entry into application, we wish to highlight and urge action to tackle the vast enforcement gap. GDPR was designed to address information asymmetries between individuals and entities which process their data and empower people to control it. Two years into the GDPR, this is still not the case. Effectiveness and enforcement are two pillars of the EU data protection legislation where national data protection authorities (DPAs) have a crucial role to play.

“Business as usual” should urgently be put to an end

In our experience as EDRi network, we have observed numerous infringements of the very principles of the GDPR but controllers are not being sufficiently held to account. The most striking infringements include:

- Abuse of consent

Consent for processing data for marketing purposes is notoriously obtained through deceptive design (“dark patterns”)¹, bundled into terms of service, or forced on individuals under economic pressure, and used to “legitimise” unnecessary and invasive forms of data processing, including profiling based on their sensitive data. Two years into the GDPR, internet platforms and other companies which rely on monetising information about people still conduct “business as usual”, and users’ weaknesses and vulnerabilities continue to be exploited. In this respect, our members found out as well that the minimization principle is often not fully enforced in the Member States, leading to abuses on the collection of personal data both by private and public entities².

- Failure of access to behavioural profiles

While internet platforms generate more and more profit from monetising knowledge about people’s behaviours, they are notorious in ignoring the fact that observations and inferences made about users are personal data as well, and are subject to all safeguards under the GDPR. However, individuals still do not have access to their full behavioural profiles or effective means of controlling them. Infringements do not only further exacerbate the opacity surrounding the online data ecosystem but also constitute a major obstacle to the effective exercise of data subjects’ rights, effectively undermining the protection afforded by the Regulation and equally citizens’ trust in the EU to protect their fundamental rights.

¹ Please see “[Deceived by design](#)” report by Norwegian Consumer Council for examples of this practice.

² See for example Xnet’s [report on Privacy and Data Protection against Institutionalised Abuses in Spain](#).

Please see the following articles for further elaboration of this problem:

[“Uncovering the Hidden Data Ecosystem”](#) by Privacy International; [“Your digital identity has three layers, and you can only protect one of them”](#) by Panoptykon Foundation.

Urgent action by DPAs is needed to make the protections in GDPR a reality

Many national DPAs do not have the financial and technical capacity to effectively tackle cases against big online companies. They should therefore be properly equipped with resources, staff, technical knowledge and IT specialists, and they must use these to take action. In this regard, we urge the European Commission to start infringement procedures against Member States that do not provide DPAs with enough resources.

Moreover, our experience as a network, through GDPR and AdTech complaints³, illustrates the urgent need for enforcement, as well as issues with a lack of coordination, a slow pace and sometimes an evasive approach of national DPAs.

Please see the following materials for further elaboration of this problem: [Response to the roadmap of the European Commission’s report on the GDPR](#) by Open Rights Group, Panoptykon Foundation and Liberties EU and [“Two years under the GDPR”](#) by Access Now.

The role of the EU Commission and of the European Data Protection Board (EDPB) when applying the cooperation and consistency mechanisms is crucial. The EDPB is an essential forum for the DPAs to exchange relevant information regarding enforcement of the GDPR. Even if we understand that not every aspect of the one-stop-shop mechanism is handled at the EDPB level, cooperation between DPAs is of the essence to complete procedures and handle complaints appropriately and promptly, in order to offer to the individuals an effective redress, in particular in cross borders cases.

Furthermore, full transparency should be afforded to the complainant, including information on the investigation made by the DPAs, copies of the reports and the possibility to take part in the procedure if appropriate.

When necessary, we urge DPAs to consider calling upon Article 66 of the GDPR and trigger the urgency procedure to adopt temporary measures, or to force other authorities to act where there is an urgent need to do so. We regret that such possibility has not yet been explored.

Derogations by Members States and DPAs

EDRi is deeply concerned by the way most Member States have implemented the derogations, undermining the GDPR protections and by the misuses of GDPR by some DPAs.

Please see Access Now’s 2019 report [“One year under the GDPR”](#) for more details.

Our concerns relate to the introduction of wide and over-arching exemptions under Article 23, removing the protections of GDPR from huge amounts of processing with consequences for people’s rights⁴. Moreover, Member States have been stretching the interpretation of the conditions set out in Article 6 and introducing broad conditions for processing special category personal data under Article 9 which are open to exploitation, including for example loopholes that can be abused by political parties.⁵

3 See our members complaints: <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem>; <https://noyb.eu/en/projects>; <https://en.panoptykon.org/complaints-google-iab>; <https://www.openrightsgroup.org/campaigns/adtech-data-protection-complaint>

4 A deeply concerning example is the immigration exemption introduced in the UK’s Data Protection Act 2018. See also Homo Digitalis complaint regarding Greek Law 4624/2019: <https://www.homodigitalis.gr/en/posts/4603>

5 See for example <https://edri.org/apti-submits-complaint-on-romanian-gdpr-implementation/>

The majority of Member States also decided not to implement the provision in Article 80(2) of GDPR allowing for collective complaints. Many of the infringements we see are systemic, vast in scale and complex, yet without Article 80(2) there is no effective redress in place since only individuals are able to lodge complaints, and not associations independently.

Moreover, there are serious concerns as to political independence of DPAs in some countries. In Slovakia⁶, Hungary⁷ and Romania⁸, DPAs are abusing the law to go after journalists and/or NGOs. In Poland the DPA has presented interpretations of the GDPR that support the government's agenda⁹. Not only is such an interpretation incorrect, but it risks being political as well as undermining the GDPR as it gives the false impression that the law infringes on free expression and media freedom. Disparities on the (lack of) implementation of Article 85 are also concerning¹⁰.

Need for complimentary and supporting legislation

GDPR does not and cannot operate in a silo. Just as the right to data protection interacts with other rights, it is essential that other legal frameworks bolster the protections of GDPR. We urge the Commission not to reopen the GDPR but we emphasise the need for complimentary and supporting legislation¹¹.

The use of algorithms or AI in decisions affecting individuals, which are not fully automated or not based on personal data, are not covered by Article 22 GDPR, despite being potentially harmful. To address this insufficiency, some of our members highlight the need for a complimentary and comprehensive legislation on such decisions.

Moreover, the upcoming Digital Services Act (DSA) is an opportunity for the European Union to make the necessary changes to fix some of the worst outcomes of the advertisement-driven and privacy-invading economy, including the lack of transparency of users' marketing profiles and of users' control over their data in the context of profiling and targeted advertisement.

Finally, EDRi and our members repeatedly stated¹², we believe that a strong and clear ePrivacy Regulation is urgently needed to further advance Europe's global leadership in the creation of a healthy digital environment, providing strong protections for citizens, their fundamental rights and our societal values.

In May 2018, EDRi and our members widely and warmly welcomed the increased protections and rights enshrined in GDPR. Now and two years on, we call on the EU Commission, EDPB, and DPAs to move forward with the enforcement and implementation of the GDPR to make these rights a reality.

6 See https://www.europarl.europa.eu/doceo/document/E-9-2020-001520_EN.html

7 See <https://ipi.media/court-orders-recall-of-forbes-hungary-following-gdpr-complaint/>

8 See <https://www.gdprtoday.org/gdpr-misuse-in-romania-independence-of-dpa-and-transparency-keywords-or-buzzwords/>

9 See https://edpb.europa.eu/news/news/2020/edpb-adopts-letter-polish-presidential-elections-data-disclosure-discusses-recent_sv

10 See for example <https://xnet-x.net/en/complaints-ec-data-protection-spanish-legislation/>

11 See part III of the report "Who (really) targets you? Facebook in Polish election campaigns" by Panoptikon Foundation [<https://panoptikon.org/political-ads-report>] for specific recommendations on changes, which should be introduced in the Digital Services Act

12 See <https://edri.org/open-letter-to-eu-member-states-deliver-eprivacy-now/>