European Data Protection Board

Sophie in 't Veld

Member of the European Parliament

Brussels, 29 January 2020

By email only

Ref: OUT2020-0004

Subject: Your letter to the EDPB of 31 July 2019

Dear Mrs in 't Veld,

I would like to thank you for your letter dated the 31st of July 2019 concerning the appropriateness of the GDPR as a legal framework to protect citizens from unfair algorithms, including the question as to whether EDPB would find it relevant to express its intention to issue guidelines on this topic.

Please find below an answer for each of the questions you raised. Please be reassured that the EDPB takes this topic very seriously and will continue to reflect on any topic that might have an impact on the right to data protection of the citizens.

Yours sincerely,

Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Does the EDPB consider that the GDPR can sufficiently protect citizens from unfair algorithms?

The EDPB is of the opinion that the GDPR is a robust legal framework to protect citizens' right to data protection. As you know, the GDPR is built in a technologically neutral manner in order to be able to face any technological change or evolution. As per its competence, the EDPB can only answer the question from the data protection perspective. It is, however, well aware that the issue of unfair algorithms may also have consequences in other areas, such as in consumer protection, antidiscrimination and competition law. Members of the EDPB have therefore continuously engaged with other relevant regulatory authorities in their member states and at EU level.

Any processing of personal data through an algorithm falls within the scope of the GDPR. This means that the GDPR covers the creation of and use of most algorithms. Thanks to - inter alia - the risk based approach, the data minimisation principle and the requirement of data protection by design and by default, the current legal framework addresses many of the potential risks and challenges associated with the processing of personal data through algorithms.

Algorithms can result unfair or even discriminatory outcomes for many reasons that need to be addressed separately because each of them may require specific levels of protection for the involved individuals. For instance, as can be the case with personalised services, discrimination can be an intentional choice of the creator of the algorithm or of the decision maker.[1] Secondly, some datasets that are collected in our current society may contain signs of biased, unjust, unfair or even discriminatory beliefs and behaviour, or simply reflect the habits of a majority of individuals, whose preferences may be perceived as unfair and discriminatory for the minority. Hence, when algorithms are trained on the basis of such biased data or on the basis of mismatches between majorities and minorities, the resulting algorithm will reflect this bias or mismatch.[2] Finally, discrimination may even come as an unintentional side effect of the design or use of the algorithm. Some of these sources of discrimination have to do with human intentions and require specific behavioural or ethical safeguards, others have to do with the way data, sometimes personal data, is processed.

In addition to the risk of unfair treatment, algorithms present two other challenges from a data protection perspective, which are inherent to the technology. Firstly, there is the incentive for processing large amounts of data: the common assumption is that the more data is used to train algorithms, the more accurate they become at predicting what they were trained to do. Apart from

[1] Gary S. Becker in "The economics of discrimination" (Milton Friedman ed., 2nd ed. 1971).

[2] For a discussion on the risks of discrimination by algorithms see 'Discrimination, artificial intelligence, and algorithmic decision-making', Prof. Frederik Zuiderveen, University of Amsterdam, Council of Europe 2018, available at https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/studies.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

questioning the general validity of this assumption[3], this "data maximization" approach creates an incentive for large and possibly unlawful data collection and further processing of data. Secondly, algorithms are becoming more and more complex, which makes them less transparent. This lack of transparency is caused by the fact that the inner workings of the algorithms are simply very difficult to understand or explain (''black box''). This can lead to a lack of transparency towards the data subject whose data is processed by the algorithm and a loss of human autonomy for those working with algorithms.

While the GDPR is applicable in its entirety to all processing of personal data, the EDPB would like to highlight specific provisions that can play an important part in addressing the potential risks arising from the use of algorithms. The general principles laid out in Art. 5 GDPR, specifically lawfulness, fairness and transparency, accuracy, data minimisation and purpose limitation govern the processing of personal data, both when creating[4] and using algorithms.

The principle of transparency, further specified in articles Art. 12-14 GDPR, requires that controllers take appropriate measures in order to keep the data subjects informed about how their data is being used. This needs to be done in a concise, transparent, intelligible and easily accessible way.[5] These provisions require anyone using an algorithm for automatic decision-making, to inform data subjects of the existence of this process and provide meaningful information about its logic, as well as the significance and envisaged consequences.[6] Furthermore, Recital 60 explicitly states that the data subject should be informed of the existence of profiling and the consequences of such profiling. Transparency is about enabling data subjects to understand and to make use of their rights in Art. 15 to 22 GDPR, if necessary. Further, it is about controllers' obligation to ensure that data subjects are not adversely impacted, including by unintentional consequences of algorithmic decisions (principle of accountability).

Furthermore, on the basis of Art. 25 GDPR, data controllers have to ensure data protection by design and by default, meaning they need to put in place appropriate measures that are designed to

---

[3] E Junqué de Fortuny, D Martens, F Provost, in "Predictive Modeling with Big Data: Is Bigger Really Better?" Big Data, 2013, vol. 1, no. 4, pp. 215–226.

[4] This can be achieved by data protection by design and by default in the creation of algorithms: EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default". Version 1.0, 13 November 2019. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

[5] Recital 39, Article art. 5(1) and art. 12-14 GDPR; for further elaboration on the principle of transparency, see the Article 29 Working Party. "Guidelines on transparency under Regulation 2016/679". WP260 rev.01, 11 April 2018 - endorsed by the EDPB. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025.

[6] Articles 13(2)(f), 14(2)(g) GDPR.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

effectively implement the aforementioned data protection principles, protect the rights and freedoms of natural persons and integrate necessary safeguards, when deciding to use or when training an algorithm. This requires a data protection oriented approach when developing the technology in the various steps of development, selection and use of algorithms.[7]

In addition, the principle of accountability requires that the controllers ensure compliance with the GDPR and are able to demonstrate this compliance.[8] This means controllers are obliged to consider all the potential risks that the use or creation of the specific algorithm can potentially pose to the rights and freedoms of natural persons and, if necessary, take measures to address these risks. While Art. 24 GDPR primarily concerns the rights to data protection and privacy, it may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, and the rights to liberty, conscience and religion.[9]

The use or development of an algorithm can trigger the obligation to carry out a Data Protection Impact Assessment (DPIA) (Art. 35 GDPR) prior to any processing taking place. If the outcome of the DPIA indicates that the processing would, in the absence of measures, result in a high risk, the controller will have to consult the relevant supervisory authority prior to the processing.[10] The outcome of the assessment can also be that the controller will have to refrain from using a specific algorithm, or parts of it, if the risks to the rights of data subjects and other persons cannot be sufficiently mitigated. All the processing activities and the measures taken to ensure compliance as described in the DPIA need to be included in the records of processing activities, which can be viewed by the supervisory authorities as part of its investigative powers.[11]

Lastly, the GDPR contains specific provisions concerning automatic decision-making. Art. 22 GDPR prohibits any decision-making based solely on automatic processing, if such a decision *'produces legal effects concerning* [the data subject] *or similarly significantly affects* [the data subject'].[12] This means

---

[7] Article 25 GDPR, EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default". Version 1.0, 13 November 2019. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en; see specifically the subsection on "fairness" in section 3.

[8]Article 24 GDPR and art. 5(2) GDPR.

[9] Art. 24 and Art. 35 GDPR; Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". WP 248 rev.01, 4 2017 - endorsed by the EDPB. https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

[10] Article 36 GDPR.

[11] Article 24 and Article 58 GDPR.

[12] Art. 22(1) GDPR. This prohibition has limited exceptions listed in Article 22(2) GDPR. See for more specific guidance on Article 22: Article 29 Working Party ''Guidelines on Automated individual decision-

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

that in practice it will often not be possible to rely solely on the outcome of an algorithm for sensitive decision-making. Furthermore, Art. 22 requires the controller to implement suitable measures to safeguard the data subject's rights and freedoms and its legitimate interests, which has to include the right to obtain human intervention.[13] This human intervention has to be qualified, capable of discovering and recovering unfair outcomes or discriminations, as the EDPB has recently pointed out in its guidelines on data protection by design and by default.[14]

Does the EDPB consider that enforcement of the GDPR in the context of algorithms is sufficient and effective, or does it consider that additional and specific legislation is necessary to better protect citizens against discriminatory algorithms, and to provide more transparency on the functioning of algorithms?

Furthermore, will the EDPB issue guidelines on what it considers a fair algorithm?

Considering the already extensive existing legal framework the EDPB considers additional legislation in the area of data protection aimed at a specific technology as premature at this time. Rather our focus at this time lies on the development of existing norms, specifically the requirements of transparency, accountability and the DPIAs in the context of machine learning algorithms. In the future, this may lead to the development of guidelines.

Taking into account that the use of 'unfair' algorithms may have consequences outside of the area of data protection, the EDPB believes that in order to protect individuals from unfair or discriminatory outcomes of algorithms an interdisciplinary approach is needed. The current legal framework for data protection does however offer many options for effective supervision and enforcement on the aforementioned aspects of fairness and transparency, and individuals' rights, granting control over their personal data by data protection authorities. This enforcement can take many forms, including, but not limited to:

- actively informing the public regarding their rights;
- engaging with stakeholders;
- informing and guiding organisations;
- assessing prior consultations and;
- carrying out investigations, which may lead to enforcement actions.

---

making and Profiling for the purposes of Regulation 2016/679'' WP 251 rev.01, As last Revised and Adopted on 6 February 2018 – endorsed by the EDPB. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[13] Art. 22(3) GDPR.

[14] EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default". Version 1.0, 13 November 2019. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Several authorities have received requests for prior consultations, informal requests for advice from organisations that include algorithmic technology and some have issued and contributed to guidance.[15] At the same time, the EDPB recognises that ensuring effective enforcement of the existing obligations under the GDPR in the context of this fast developing technology will continue to require considerable and continuous investment in up-to date expertise and sufficient resources in the coming years.

[15] See https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/ai-and-privacy/ (Norwegian Data Protection Authority); https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/ (UK Data Protection Authority); https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues (French Data Protection Authority) https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html (Germany's Federal Date Ethics Committee (Datenethikkommission)) ; https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf (International Working Group on Data Protection in Telecommunications); http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf (International Conference of Data Protection and Privacy Commissioners).

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels