BRIEFING
STOA Options Brief

European Parliament

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence

Although artificial intelligence (AI) is not explicitly mentioned in the EU General Data Protection Regulation (GPDR), many of its provisions are relevant to the use of AI, and some indeed face challenges posed by the new ways of processing personal data that are enabled by AI.

A tension exists between traditional data protection principles – purpose limitation, data minimisation, special treatment of 'sensitive data', limitations on automated decisions – and the full deployment of the power of AI. However, it is possible to interpret, apply and develop those data protection principles that are consistent with beneficial uses of AI.

A number of AI-related data-protection issues are not explicitly answered in the GDPR, where provisions are often vague and open-ended. Controllers and data subjects should be provided with guidance on how AI can be applied to personal data in conformity with the GDPR, and on the available technologies for doing so.

A broad social, political and legal debate is needed on what standards should apply to processing of personal data using AI, particularly to ensure the explanation, acceptability, fairness and reasonableness of decisions about individuals. The debate should also address the question of which applications are to be barred unconditionally, and which ones may instead be admitted only under specific circumstances and controls.

Figure 2 – AI and big data: Challenges to GPDR

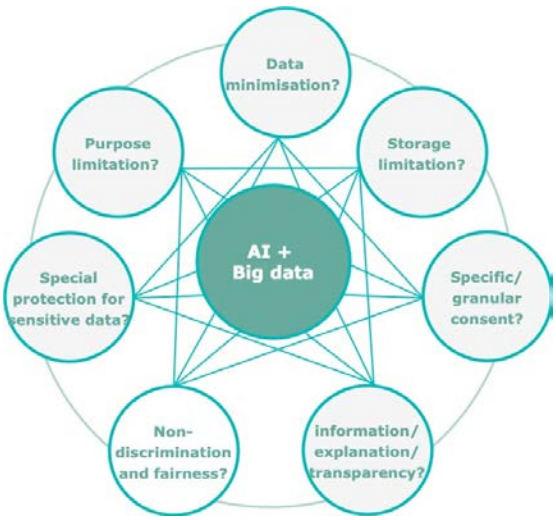

Figure 1 – AI and big data: Goals for GDPR

1. Regulatory options

The EU General Data Protection Regulation (GDPR) provides significant and purposeful guidance for data protection in the context of AI applications; no major changes to the GDPR are needed in order to address AI. However, a number of AI-related data-protection issues are not explicitly answered in the GDPR. This may lead to uncertainties and costs, and may needlessly hamper the development of AI applications. Indeed, the GDPR abounds in vague clauses and open standards, such as: 'personal data concern identified or *identifiable* natural persons' (Article 4(1)); 'consent must be *freely given*' (Article (4)(11); 'further processing must be *non-incompatible* with the original processing' (Article 5(1)(b)); 'the data must be *necessary* for the purposes for which they are processed' (Article 5 (1)(c)); 'controllers must pursue *legitimate* interests that are *non-overridden* by the interests or fundamental rights and freedoms of the data subject' (Article 6(1)(f)); 'the information about the logic involved in automated decision-making must be *meaningful*' (Articles 13(2)(f) and 14 (2)(g)); '*suitable* safeguard measures should be adopted for automated decision-making' (Article 22 (2)); 'technical and organisational measures for data protection by design and by default must be *appropriate*' (Article 25). It may be difficult for controllers to determine whether the processing they envisage satisfies these open standards.

Moreover, in various cases, applying GDPR standards requires balancing competing interests. To determine whether a certain processing activity is admissible, or whether a preventive measure is to be adopted, it must be established whether the controllers' interest in processing the data and in not adopting certain measures is outweighed by the data subjects' interest in not being subject to the processing or in being protected by additional or stricter measures. These assessments depend on both (a) uncertain normative judgements about the comparative importance of the impacts of the envisaged processing or measure on the interests at stake, and (b) uncertain forecasts concerning potential future risks. In the case of AI, the uncertainties involved in applying indeterminate concepts and balancing competing interests are aggravated by the novelty of the technologies, their complexities, and the broad scope of their individual and social effects.

By requiring controllers to apply these indeterminate principles, the GDPR offloads the task of establishing how to manage risks and find optimal solutions onto controllers, a task which can be challenging as well as costly. Stiff penalties for non-compliance, coupled with uncertainty about what is required for compliance, may constitute a novel risk, which, rather than incentivising the adoption of adequate compliance measures, may prevent small companies from engaging in new ventures. In the absence of adequate guidance, there are two parallel risks: big players may profit from the uncertainty, by adopting solutions that go against the spirit of the GDPR, while small companies may refrain from availing themselves of opportunities that are consistent with the GDPR.

Thus, the impact of the GDPR on AI in Europe will critically depend on what guidance controllers and data subjects receive from the competent authorities, as well as from civil society, academic institutions and politically accountable bodies. Appropriate guidance would diminish the cost of legal uncertainty and would point companies – smaller ones in particular – to efficient and data-protection compliant solutions.

Among the clarifications needed, the following are particularly relevant.

Personal/inferred data. It should be clarified that inferred personal data count as newly collected personal data (Article 6), when used as input for profiling, assessments, and decisions. The same should apply to the re-identification of anonymous (de-identified) data. Clarifications are needed concerning the extent to which the abstract possibility of using AI techniques for re-identification may lead to de-identified data being considered as still personal.

Data protection principles. It should be specified how data protection principles – and in particular the principles of purpose limitation, data minimisation and storage limitation (Article 5 GDPR) – apply to AI systems. The implementation of such principles must be made consistent with the need to process large datasets to extract useful algorithmic models, as well as with data subjects' rights.

Legal basis. It should be clarified that the construction of algorithmic models based on personal data for useful social applications is generally compatible with the requirement that the processing have a legal basis (Article 6). However, the personal data should be pseudonymised and anonymised as soon as possible, and risk-prevention measures must be adopted.

Statistical processing. Statistical processing of personal data, not leading to individualised inferences, is in principle allowed and should be encouraged, as long as appropriate precautions are in place preventing abuse, and as long as the data are pseudonymised or de-anonymised at the earliest possible moment. The enactment of appropriate measures at the national level should be promoted. It would be useful to specify what statistical processing is unacceptable.

Explanations. It should be made clear that controllers have best-effort obligations to provide data subjects with individualised explanations when their data are used for automated decision-making: these explanations should specify what factors have determined unfavourable assessments or decisions (Article 22, Recital 71). This obligation has to be balanced with the need to use the most effective technologies. Explanations may be high-level, but they should still enable users to contest detrimental outcomes.

Reasonableness of inferences. Criteria should be clarified for the acceptability of automated inferences whenever the outcomes of such inferences are to be acted upon. These include normative requirements as well as statistical-logical soundness.

Facilitation and standardisation of the exercise of data subjects' rights. The rights to object to and opt out of AI-based processing can be easily exercised by data subjects through appropriate user interfaces, possibly in standardised formats (Article 21) need to be ensured. Whenever the data subject has a right to opt out, opting out should not be more difficult than opting in. Similarly, the effective, explicit and free exercise of data subjects' consent (or denial of consent) to AI-based processing is to be ensured whenever consent may provide a legal basis.

Collective enforcement. Collective enforcement in the data protection domain should be facilitated, in particular by enabling collective actions for injunctions and compensation. The proposed directive on collective redress for consumers could be taken as an opportunity to begin tackling this issue.

Data protection by design and by default. The preventive measures needed for different kinds of AI applications should be specified: these measures should be designed to ensure, among other things, that training sets are representative and inferences are reasonable, as well as that the processing is free of unfairness and discrimination, and also secure (Article 25).

High-risk processing. Which AI applications constitute high-risk processing, and thus require a data-protection impact assessment and the involvement of a data protection officer should be more clearly specified. Whether all assessments concerning AI applications (possibly with some exceptions) should be communicated to the competent supervisory authority (Article 35) ought to be considered. It should also be determined which larger and riskier types of processing should require certification (Article 25).

Prior consultation. The possibility to request a prior opinion from the supervisory authority may be extended to all AI-based applications involving the processing of personal data. The cases in which a prior opinion is mandatory should be more clearly defined (Article 36).

Socially unacceptable or dangerous applications. Socially unacceptable or dangerous applications should be identified, and their use excluded or restricted, even when they meet fairness and scientific requirements.

2. Procedural options

Procedural options include policy options aimed at enhancing processes and established practices relating to data protection in the context of AI.

Encouraging public debate. A broad debate on AI and data protection is needed involving not only political and administrative authorities, but also civil society and academia. This debate should consider what standards may apply to the AI-based processing of personal data, particularly to ensure the acceptability, fairness and reasonableness of decisions about individuals. Discussion of a large set of realistic cases is needed to clarify which AI applications are, on balance, socially acceptable and under what circumstances and constraints. The debate on AI can also provide an opportunity to reconsider in depth, and with greater precision and concreteness, some basic ideas of European law and ethics, such as acceptable and workable models for fairness and non-discrimination.

Restricting AI applications. A policy debate should address the question of which applications are to be barred unconditionally, and which ones may instead be admitted only under specific circumstances. Novel guidance is needed to this effect, since the GDPR focuses on individual rights and does not take into account the broader social impacts of mass processing.

Guiding controllers and data subjects. Controllers and data subjects should be provided with guidance on how AI can be applied to personal data in conformity with the GDPR, and on the technologies available to that end. Such guidance can prevent costs linked to legal uncertainty, while enhancing compliance.

Providing guidelines. Guidelines should be developed to help controllers and data subjects navigate compliance with the GDPR in the context of the use of AI. The involvement of the European Data Protection Board and of national supervisory authorities is essential, as is participation from academia. The guidelines should indicate preferred practices and suggest adequate technological solutions, to ensure that AI-based processing is a positive-sum game. They should also identify detrimental practices involving unacceptable risks, and in particular 'dark patterns' meant to mislead or deceive data subjects, betraying their trust.

This document is based on the STOA study on 'Impact of the General Data Protection Regulation on artificial intelligence' (PE 641.530) published in June 2020. The study was written by Professor Giovanni Sartor of the European University Institute of Florence, at the request of the Panel for the Future or Science and Technology (STOA) and managed by the Scientific Foresight Unit within the Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament. STOA administrator responsible: Mihalis Kritikos.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2020.

stoa@ep.europa.eu (contact)

http://www.europarl.europa.eu/stoa/ (STOA website)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)