

## 9 Executive Summary

The General Data Protection Regulation (GDPR) has improved the standing of consumers regarding the processing of personal data in many places. Examples are the residence principle, the right to data portability, data protection by design, the right to lodge a complaint and the sanctioning of violations.

Yet, it does not realise its full potential. On the one hand, the GDPR has created significant legal uncertainty, which often affects consumers adversely. This uncertainty results mostly from the fact that the GDPR remains abstract and omits clarifying specifications – both concerning its understanding and its practical implementation. This entices providers to use the existing room for manoeuvre to the disadvantage of consumers. On the other hand, certain consumer-friendly provisions simply were unsuccessful during the creation of the GDPR. This concerns for instance an adequate protection from scoring. Both hinder the innovations that the GDPR aimed to introduce 2018 into the European data protection practice. They are unable to unfold their potentials when it comes to protecting consumers.

This report shows that issues exist on two levels. First, there are issues that result from deficits in the text of the regulation. Here, the report suggests 33 alterations of the text in order to improve it – from the point of view of consumers. Beyond that, there are conceptional issues that cannot be resolved with smaller alterations of the text of the norm. The report suggests and discusses approaches to these issues whose implementation is directed more towards the future.

Considering these expectations, the evaluation report of the European Commission from 24 June 2020 is underwhelming. It is limited solely to select issues of the implementation of the GDPR and rejects any discussion of the improvements of the text of the regulation that were proposed in many written comments. And yet, the evaluation of the GDPR would have been presented the ideal opportunity to point out these issues to European Union lawmakers and to present proposals that constructively evolve the GDPR. The goal must be to reduce the power gradient between providers and consumers. This goal is achieved by better bringing to bear the innovations that are laid out already in the GDPR.

The success of the consumer-friendly innovations of the GDPR must not solely depend on the interpretation of the applicable text from 2016. Instead there need to be specifications that anchor provisions that are more friendly to fundamental right and that frame the rights of consumers and the obligations of controllers more clearly directly in text of the relevant articles of the GDPR. Even small changes of the text can achieve the necessary specifications or at least significantly increase the clarity of existing provisions and strengthen the position of consumers. Where this is not the case, instead of the EU lawmakers, the lawmakers of the member states, the European Data Protection Board and the national data protection authorities need to enact laws or guidelines. The report contains proposals regarding this as well.

In particular, the report proposes the following revisions of the GDPR. The sequence of the recommended revisions is not meant to indicate a prioritisation of certain revisions.

Processing in the course of a purely personal or household activity:

- Retraction of the complete exemption of invasive data processing from the material scope of the GDPR in Art. 2(2)(c); instead risk-adequate differentiation also in the context of personal or household activity; complete exemption from the material scope only for low-risk processing; for heightened risks application of select provisions of the GDPR.

Residence principle:

- Expansion of the territorial scope of the GDPR to include every type of processing of personal data of data subjects that reside in the European Union.

Principles relating to processing of personal data:

- Adjustment of the German language version of the GDPR: Replacing the term “Treu und Glauben” in Art. 5(1)(a) with “Fairness”.
- Amendment of the GDPR with an obligation to data avoidance in Art. 5(1)(c).
- Modernising and risk-adequate evolution of the principles.

Relations between consent and other grounds for lawful processing:

- Clarification in Art. 6(1)(1) GDPR that a controller in addition to consent or as substitute for consent cannot rely on another ground for lawful processing while creating different legal effects on the data subject.

Determining the purpose of a contract:

- Specification of Art. 6(1)(1)(b) GDPR: objective (functional) specification of the processing of personal data that is necessary to fulfil a contract independently from the phrasing of the contract.

Profiling:

- Separate provisions on lawfulness regarding profiling, which shall be unlawful by default and only possible in pre-defined exceptions.

Processing of data of children:

- Consideration of the special protection that children merit when assessing the compatibility of a new purpose with the initial purpose, if the data of a child are to be used for another purpose.
- Transfer of recital 38(2) GDPR to the articles, prohibiting the use of personal data of children for the purposes of marketing or profiling.
- Exclusion of the consent of a child from the processing of special categories of personal data according to Art. 9(2)(a) GDPR.
- Special consideration of the fact that personal data has been obtained during childhood in the right to object.
- Inadmissibility of the consent of a child to the processing of personal data for automated individual decision-making.
- Special consideration of the fundamental rights and interests of children in the context of data protection by design and by default according to Art. 25 GDPR.
- Incorporation of an obligation to special consideration of the fundamental rights and interests of children in the context of risk analysis and when determining measures for protection during a data protection impact assessment.

Presenting information:

- Addition of specific provisions regarding the presentation of information in the context of specific fields of processing and technologies.
- Presentation of information that is adequate to the situation, the interests and the decisions involved.
- Focussing of information on the actual circumstances of the respective processing that is about to occur.

Information to be provided by the controller:

- Addition of a basic rule to resolve the conflict between the right to access and the protection of trade secrets: provision of the highest amount of information possible while protecting trade secrets and intellectual property; obligation to provide a maximum of information while still taking these opposing interests into account.
- Clarification that information on the “logic involved” entails the criteria for the decision and their balancing.
- Clarification that a division of labour or cooperation in the context of automated individual decision-making must not lead to an omission or limitation of information to be provided to the data subject; obligation

to inform about divided / cooperative automated decision processes that has to be met by every cooperating partner concerning his or her contribution to the process including the interfaces to all other contributions.

- Addition of an obligation to provide information for every profiling, even if it is not directly linked to an automated individual decision but is instead used for other assessment purposes.
- Amending Art. 13 GDPR with rules that facilitate the provision of information in everyday contact/communication.

Right of access by the data subject:

- Obligation of the controller to log all recipients of personal data; obligation to present the contents of the log to the data subject.
- Obligation of the controller to separately inform the data subject of any profiling, its extent, contents, goals and purposes.
- Specification of the right to be provided with a copy; addition of an obligation to communicate all processed data wherever no copy can be provided.

Right to data portability:

- Rephrasing the title of the norm in a way that not only describes a possibility, but the action that the consumer may demand, and that the controller is obligated to perform: “Recht auf Datenübertragung” / “right to data transmission”.
- Expansion of the right to data transfer to the data caused by the data subject.
- Stipulation of the transfer of data in an interoperable format and in German (or the respective language of the member state) or in English.

Automated individual decision-making:

- Deletion of the limitation “solely” in the scope of the applicability of the provision.
- Addition of a prohibition to be subjected to automatically prepared decisions that the human decider adopts without review and without giving the data subject the opportunity to present his or her point of view prior to the decision.
- Deletion of the limitation that the decision must produce legal effects concerning the data subject or “similarly significantly affects him or her”; a detrimental effect shall be sufficient.
- Deletion of Art. 22(2)(a) GDPR. Processing on the basis of consent of the data subject according to Art. 22(2)(c) is sufficient.

- Addition of qualitative requirements for a decision that is based on an automatically prepared decision in the image of § 31 of the German Federal Data Protection Act.
- Amendment of Art. 22(3) GDPR with the phrase “to clarification of the reasons for the decision”.

Responsibility of the controller:

- Addition of a liability for manufacturers to support the controller.

Data protection by design:

- Addition of an obligation to award special protection to the fundamental rights and interests of children.
- Technologically specific or sector-specific specification of the obligation of data protection by design by the Board.
- Expansion of the obligation to producers/manufacturers of systems that process personal data.

Data protection by default:

- Limitation of the purpose to the functionality of the respective service.
- Amendment of the principle of data avoidance.
- Addition of an obligation to award special protection to the fundamental rights and interests of children.

Powers of the supervisory authorities:

- Amendment of the powers of the supervisory authorities in Art. 58(1) and (2) GDPR with the power to instruct manufacturers.

Tasks of the European Data Protection Board:

- Incorporation of additional tasks of the European Data Protection Board in Art. 70(1) GDPR: Specification of the obligation to data protection by design according to Art. 25(1) GDPR and data protection by default according to Art. 25(2) GDPR as well as specification of interoperable formats for a transmission of data following Art. 20(1) and (2) GDPR.

Remedies and penalties with regard to manufacturers:

- Extension of the right to an effective judicial remedy and the right to receive compensation to manufacturers.

Regarding administrative fines:

- Specification of the provisions on administrative fines through guidelines issued by the Board in accordance with Art. 70(1)(2)(k) GDPR; specification through non-binding catalogues on fines by the data protection authorities of the member states.
- Amendment of Art. 83(4)(a) GDPR with a cross reference to the responsibilities of the manufacturer.

- Obligation of the data protection authorities to publish an annual statistic on the issuing of fines.

The innovations of the General Data Protection Regulation can only unfold, if sufficiently concrete provisions ensure an effective application. Legal uncertainty must be avoided. However, in many places the GDPR goes too far in the direction of openness and thus prevents – for lack of specification – that legal obligations are taken seriously, and that data protection is appreciated in all its facets. The success of the innovations of the GDPR depends on these specifications. This report has made recommendations how to improve the GDPR with regard to its consistency and implementation in order to constructively advance the regulation. While drafting these recommendations, the view of the consumer took centre stage. Strengthening the position of the consumer and to reduce the asymmetry of power between controller and data subject is in line with the pronounced goal of the GDPR to have the processing of personal data serve mankind, to safeguard the fundamental rights and freedoms of data subjects and to contribute to the well-being of natural persons – indeed with respect to the rights of the controllers.

This report has demonstrated that even small changes in the wording of the provisions of the regulation can have a significant effect in strengthening the position of consumers and to prevent aberration. In some places however, extensive specification and clarification through guidelines issued by the European Data Protection Board is irremissible.

The recommendations given could have already been used in the context of the evaluation of the GDPR in the year 2020 for constructive enhancements of the regulation. Some of the recommendations would likely have sparked opposition and required a comprehensive discussion in the European Union. Others however are so clear and simple that they can hope for broad consent. The fact that the Commission did not seek to consider or at least to discuss them in the evaluation report does not call their eligibility into question. They can and will provide the basis for a continued discussion on necessary improvements of the GDPR.

Data protection law governs a field of law that is challenged constantly and profoundly by emerging business models and the dynamic evolution of information technology. Therefore, the GDPR cannot be the final act in the discussion on the structural foundation and implementation of data protection law. Rather, developments are on the horizon that simply overstrain the current data protection law. The reason for this is on the one hand that the GDPR in essence maintains the fundamental concepts of data protection law that were developed in the 1970s. On the other hand, it

results from the refusal of the EU lawmakers to enact technologically specific basic rules that do justice to the biggest threats to fundamental rights caused by modern information technology. The report offers food for thought regarding these fundamental questions and outlines approaches that prevent disadvantages for consumers in the context of the risks that emerge from these challenges.