Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection
EAID

Berlin, 27 January 2020

Evaluation of the General Data Protection Regulation

Contents

Europäische Akademie für Informationsfreiheit und Datenschutz e.V.
Vorstand: Peter Schaar * Dr. Alexander Dix * Karsten Neumann * Prof. Dr. Alfred Büllesbach * Dr. Dennis-Kenji Kipker
Geschäftsstelle: Bismarckallee 46/48 * D-14193 Berlin * Telefon: +49 151-62914576
E-Mail: gf@eaid-berlin.de * www.eaid-berlin.de
Vereinsregister-Nr. VR 21680 B Amtsgericht Charlottenburg * Steuer-Nr. 27/664/52926
IBAN DE84 1005 0000 0190 3076 92 * BIC BELADEBEXXX * Berliner Sparkasse

A. General remarks

Article 8 of the EU Charter of Fundamental Rights (EUCFR) guarantees the protection of personal data and requires independent data protection oversight. With the General Data Protection Regulation (GDPR), there has been one EU data protection law directly applicable in all Member States since 25 May 2018. The extent to which the goals of the GDPR have been achieved cannot yet be seriously assessed after only 18 months. According to Art. 97 GDPR, the European Commission is required to continuously review the application and effectiveness of the Regulation and to report on this for the first time on 25 May 2020 and, if necessary, to submit proposals for amending and further developing the Regulation.

There is no denying that the GDPR has advanced the harmonisation of European data protection law and its application compared to the largely fragmented previous legal situation. The regulation has also strengthened the data protection rights of individuals subject to the processing of their data. The GDPR also provided data protection supervisory authorities with effective means of enforcement. However, it has become apparent that there are still shortcomings in the areas described above which need to be remedied.

The GDPR has had a significant impact on the global debate on data protection issues. Several non-European countries and federal states have now passed laws based on the model of the GDPR. Examples include the Californian Consumer Privacy Act (CCPA), which came into force on January 1, 2020, and the new Thai Data Protection Act. The US Congress has received several drafts for a federal data protection act. It is currently discussing them on a bipartisan basis. In addition, the data protection agreement concluded between the European Union and Japan in early 2019 has created the world's largest zone with a uniformly high level of data protection. This has improved the opportunities for the European economy to remain competitive in the face of ongoing digitization.

The present opinion is based on the experience gained so far and is therefore provisional in nature. It is focused on key areas of action in which further development of the legal framework already appears appropriate.

B. Proposals

1. Harmonisation

The large number of **opening and concretisation clauses** in the GDPR urgently needs to be reviewed with a view to reducing them. As a result of the fact that the Member States have made use of national options in very different ways, a regulatory patchwork of the most diverse provisions continues to exist in many areas. This severely compromises the goal of harmonising data protection law in the EU as far as possible and the associated free movement of data. Moreover, fragmentation causes considerable practical and legal problems for legal practitioners.

1.1. The opening clauses of the GDPR for **processing by public authorities** allow not only for more precise regulations in the law of the Member States, but also for clarification by Union law. The legal requirements for such regulations, such as those in Article 6 (3) GDPR and Article 9 (2) GDPR, should be specified with regard to the particular relevance of data processing by public authorities to fundamental rights in such a way that the guarantees specified in the GDPR may only be deviated from in favour of the persons concerned. In addition, so far there are Europe-wide references, the EU legislator should make greater use of its power to specify in order to further develop the principles of the GDPR in a harmonised manner for the public sector.

1.2. The diversity of regulations is particularly serious in the research field. The application of the provisions on **scientific research** has shown the need for more integrated rules on processing for scientific purposes, in particular for European cross-border research. Art. 89 GDPR should be revised accordingly in order to ensure a uniformly high level of data protection throughout the EU.

1.3. A higher degree of harmonisation is also needed for the processing of personal data in the **employment context**. The requirements for employee data protection of Art. 88 GDPR should be designed as binding guidelines for the processing of employee data and not merely as an option for national legislators. Nevertheless, it should still be possible to specify the requirements in national law and collective agreements.

1.4. In view of the increasing importance of interactive, cross-border media, more binding and concrete criteria are needed for weighing up the relationship between data protection, **free speech and freedom of information**. Art. 85 GDPR should be further developed accordingly.

1.5. The **cooperation of DPAs** is crucial for the uniform application of data protection law. The principles set out in Chapter VII (Art. 60-78) GDPR must be made more effective. There is a need for legal remedies if a supervisory authority fails to take a decision pursuant to Art. 58 in cases of cross-border importance, delays it, or intends to refrain from taking a formal measure pursuant to Art. 58 (2) GDPR with a view to amicably resolving a dispute with the company. It must be ensured by corresponding changes in Art. 64-66 GDPR that the provisions on the coherence procedure also apply to such cases.

2. Profiling / Automated decisions

Greater attention must be paid to automated systems which make or prepare decisions important for the individual or for society. Of particular relevance in terms of data protection law is the compilation and evaluation of data for the purpose of assessing individuals (profiling) and the use of algorithmic decision-making systems, for example in connection with the use of "artificial intelligence" (AI).

2.1. Art. 22 GDPR should be adapted to cover all cases where the rights and freedoms of natural persons are **significantly affected**. Profiling must be regulated as such (and not just decisions based on it). It should be clarified that the rules for automated decision-making also apply to decisions that are essentially based on algorithmic systems (algorithmic decisions). In this respect, **absolute limits** must be defined, admissibility requirements must be standardised and the principle of proportionality must be specified. In doing so, the specific requirements for the use of sensitive data and for the use of **data relating to children** shall be taken into account. The transparency requirements of Art. 12 et seqq. for profiling and automated decisions should be formulated more specific. Persons affected must always be informed when profiling is carried out and what the consequences are. In the case of algorithmic and algorithm-based

decision-making systems, the underlying data and their weighting for the specific case must be disclosed in a comprehensible form.

2.2. With regard to the **functioning and effects** of algorithmic and algorithm-based decision systems, in particular to avoid discrimination effects, mechanisms of algorithm control should be implemented. The requirements for data protection impact assessment formulated in Art. 35 (7) GDPR should be specified accordingly.

3. Data protection technology

In addition to written law, ensuring effective data protection is largely determined by the design of technical systems. The statement "Code is Law" (Lessig) applies more than ever in view of increasingly powerful IT systems and global processing. It is therefore all the more important to ensure that technical systems are designed in a way compatible with data protection, especially with regard to limiting the scope of personal data processed (data avoidance, data minimisation). Anonymisation and the use of pseudonyms are effective techniques for limiting risks to the fundamental rights and freedoms of natural persons, without unduly restricting the knowledge that can be gained from the data processing. In view of the high speed of innovation, it is necessary to examine to what extent the legal requirements guarantee adequate protection.

3.1. The provisions on **technological data protection** (Art. 25 GDPR) should take into account the particular risks arising from the use of new technologies and business models (in particular artificial intelligence, data mining, platforms). Corresponding specifications for the design of such systems should be specified by the European Data Protection Board.

3.2. In view of the rapid technological development, the requirements for **anonymisation and pseudonymisation** in Art. 25 GDPR and for the use of anonymised data should be made more specific. This should be supplemented by prohibitions of de-anonymisation and the unauthorised dissolution of pseudonyms, with the possibility of criminal prosecution.

3.3. The **responsibility of the manufacturers** of hardware and software should be increased, for example by extending the definition of the responsible person to include the natural or legal person, public authority, agency or other body marketing file systems or personal data processing services. At

the very least, they should be included as addressees of the rules on data protection by means of technology design and by means of privacy by default, Article 25, and security of processing, Article 32 GDPR, in addition to the controller and processor, with the consequence that providers of personal data processing systems and services are responsible and liable for the implementation of the requirements at the time of placing on the market. In particular, they are to be legally obliged to provide all information required for a data protection impact assessment prior to the conclusion of a contract and all information and means necessary for the implementation of the rights of the persons concerned, irrespective of company and business secrets. This could also make the provisions on **certification** under Art. 42 effective. Consideration should also be given to extending the regulations on liability and compensation (Art. 82 GDPR) and on sanctions (Art. 83 f) to manufacturers.

4. Rights of data subjects / self-determination

Self-determination and the rights of the persons concerned by the processing are at the centre of the fundamental right to data protection and the fundamental right to informational self-determination established by the Federal Constitutional Court. Although the GDPR standardises the central possibilities of influence of the individual on the processing of his or her data and his or her rights vis-à-vis the responsible parties, the actual possibilities of influence of the data subjects are often very limited. This applies in particular to the practice of various powerful companies offering services in which data subjects are trapped by lock-in effects. The rights of those affected should therefore be further strengthened.

4.1. The rules on **consent** (Art. 7 GDPR) and the **right of objection** (Art. 21 GDPR) must be supplemented in such a way that the persons concerned can make use of technical systems to determine their data protection preferences when exercising their decision-making powers. Those responsible must be obliged to respect these specifications and the decisions based on them.

4.2. In Art. 12 ff GDPR it must be ensured that the **information provided for the data subject** relates to data processing actually intended. It should also be clarified that the controller must inform the data subject of all known recipients to whom personal data of the data subject are or have been disclosed. In addition, the person responsible must be obliged to

record the transmission of the data and the recipients, so that he cannot evade his obligation to provide information on the grounds of "lack of knowledge".

4.3. The **transparency** obligations pursuant to Art. 12 et seq. are to be specified with regard to the use of profiling techniques and algorithmic decision-making procedures (cf. point 1, 2nd indent above).

4.4. The right to **restriction of processing** (blocking) in Art. 18 GDPR should be extended to those cases in which the necessary deletion is not carried out because the data must be kept only for the purpose of complying with retention periods.

4.5. The right to **data portability** (Art. 20 GDPR) should be specified in such a way that the data must be made available to the data subject in an interoperable format. It should also be ensured that the right covers all data processed by automated means that the data subject has generated (including metadata) and not only those that he has deliberately entered into a system. Furthermore, companies and platforms with a high market penetration should be obliged to make their offerings interoperable by providing interfaces with open standards.

C. Evaluation of the legal framework

Article 97(1) of the DS-GVO provides for an evaluation of the GDPR after 25 May 2020 at four-year intervals. In view of the rapid technical development in the field of data processing, it appears necessary to shorten this evaluation interval to two years. Even if the legal framework is designed to be technologically neutral, it must react to technical developments as quickly as possible otherwise it will fast become obsolete.