Gesellschaft für Datenschutz
und Datensicherheit (GDD) e.V.

GDD statement on the development of the GDPR

According to Art. 97 para. 1 GDPR, the EU Commission shall submit a report on the evaluation and review of the Regulation to the European Parliament and the Council by 25 May 2020 and every four years thereafter, which shall also be made public. In connection with the second review report due in mid-2024, the EU Commission is currently conducting a consultation on the evaluation of the General Data Protection Regulation (GDPR), which has been in force since 1 May 2018. Feedback can be submitted to the Commission until 8 February 2024. A questionnaire from September 2023, which was used to consult a so-called High-Level Expert Group, was also taken into account.

The following explanations deal with the assessment of individual areas of the GDPR that the GDD considers to be particularly worthy of consideration:

1. exercise of data subject rights

Overall, most companies are well aware that data subjects' rights are being asserted and that the corresponding requests from data subjects must also be fulfilled. Often, however, neither the data subjects nor the data controllers are aware of the extent to which the corresponding rights must be fulfilled. One of the reasons for this is that the data subjects are not always aware that the rights of data subjects are not absolute rights, but that the fulfilment of these requests can always be weighed up against the rights of others by the controller.

a) Duty to provide information, Arts. 13, 14 GDPR

The information obligations to be fulfilled by the controller in accordance with Arts. 13 and 14 GDPR have led to an excess of information that is neither requested nor taken note of by the data subject. This prevailing implementation of the information obligations in practice does not fulfil the requirement of transparency if the controller is only concerned with fulfilling its legal obligation to provide information. It would therefore be advisable to standardise further exceptions for Art. 13 and 14 GDPR and to consider standardising privacy policies on websites.

There are also certain ambiguities and uncertainties regarding the time of information. The form and deadline rule of Art. 13 GDPR is not very realistic, particularly with regard to the collection of personal data in specific everyday situations. In personal contact, when exchanging business cards, when making initial contact by email or the collection of data over the phone, the wording of Art. 13 GDPR requires the information to be provided at the time of collection. However, this would often thwart the first (personal) contact with bureaucratic transparency obligations. This could be remedied by a short, specific deadline, possibly with a penalty.

b) Right to information, Art. 15 GDPR

For data controllers, the extent to which a request for information must be fulfilled is not clearly specified. Due to its codification in Art. 8 para. 2 sentence 2 of the Charter of Fundamental Rights (CFR), the right to information is probably to be qualified as the core right of data subjects. Therefore, in order to guarantee this right, the differences between "access to such personal data" (Art. 15 para. 1 sentence 1 GDPR), information on "the categories of personal data undergoing processing" (Art. 15 para. 1 sentence 1 lit. b GDPR) and the "copy of personal data" (Art. 15 para. 3 sentence 1 GDPR) must be clarified. In legal practice, it is difficult to understand where the difference should lie in the information requested by the applicant. The term "copy" under Art. 15 GDPR in particular is associated with immense legal uncertainty due to the lack of a legal definition or concretisation in the recitals of the GDPR, as controllers currently do not know how they should respond to a request for a copy of personal data. The cooperation of the data subjects already contained in recital 63 GDPR, "that the data subject specifies the information or processing operations to which his or her request for access relates", should be codified in Art. 15 GDPR in the mutual interest of the controller and the data subject. This requirement for the data subject to cooperate in the request for information should also be specified. This specification would also mean that controllers would have clarity about when a request from a data subject has been completed.

Small and medium-sized enterprises (SMEs) regularly need more time to provide information. One reason for this is that the resources of SMEs are limited, and they often rely on outsourced processing models. Accordingly, the development of a guideline for the GDPR-compliant fulfilment of the right to information for SMEs could be the right approach to support and relieve the burden.

c) Erasure, Art. 17 GDPR

The request for erasure is becoming increasingly important and is being used more and more frequently by data subjects. However, data subjects often lack the awareness that certain data cannot be completely erased due to existing retention obligations. In addition, almost all deletions must be carried out manually to ensure that all data has actually been deleted correctly, which ties up a lot of time and resources. In this respect, the development of guidelines for the deletion of user-generated data would be beneficial.

d) Consent

The requirements for " informed consent" within the meaning of Art. 6 para. 1 lit. a) GDPR is in need of concretisation and requires a clear distinction from the duty to inform within the meaning of Art. 13 and 14 GDPR. According to Art. 5 para. 1 lit. a) GDPR, the processing of personal data must not only be lawful, but also transparent. Incorporating the requirement of transparency into the legality requirement and additionally complying with the general information obligations creates difficulties for legal practice in obtaining consent in a legally compliant manner.

e) Data portability

The right to data portability (Art. 20 GDPR) aims to ensure that the data subject is provided with data concerning him or her that he or she has provided to a controller in a format that

allows it to be transferred to another controller. This data subject right thus aims to enable or facilitate a change of provider. In the European Commission's proposal, Recital 55 GDPR cited the transfer from one social network to another as an example. With regard to the typical use case of Art. 20 GDPR, the transfer of one's own profile from one service provider on the internet (e.g. a social network or an email provider) to another, the scope of application of the regulation of Art. 20 GDPR appears too extensive. It would therefore seem sensible to limit the scope of application to (online) portals in order to fulfil the original objective of this regulation. Even if the scope of application of Art. 20 GDPR is restricted, the right of access under Art. 15 GDPR still fulfils the function of providing the data subject with transparency about their personal data upon request.

2. commissioned data processing, Art. 28 GDPR

Processing on behalf of a controller (Art. 28 GDPR) is a key legal concept for legal practice. For this reason, the specific form of the provision in Art. 28 GDPR is highly relevant for the legal practitioner. It therefore seems desirable to clarify that the written authorisation of additional processors pursuant to Art. 28 para. 2 sentence 2 GDPR can also be given electronically. In Art. 28 para. 9 GDPR, the GDPR only permits an "electronic format" for Art. 28 para. 3 and 4 GDPR. For a large number of practically relevant commissioned processing operations, the electronic form permitted by para. 9 is at risk of being rendered meaningless. This circumstance appears to run counter to the specific regulatory intention of the provision. Even if it is already correctly assumed in the application of the law that a written authorisation within the meaning of para. 2 sentence 1 GDPR can also be granted and documented in electronic format, the legislator should close this loophole in Art. 28 para. 9 GDPR if possible. This would also be achieved through a generally applicable equivalence of written and electronic form - as in Art. 28 (9) GDPR - within the definitions in Art. 4 GDPR.

3. data protection officer

According to Art. 37 para. 1 lit. a) GDPR, every public body must appoint a data protection officer, regardless of the size of the organisation and the risk of the personal data processed therein. In the private sector, however, the obligation to appoint a data protection officer remains merely the exception. In terms of a consistent focus of the GDPR on the risk-based approach, the adoption of an appointment obligation for data protection officers in the non-public sector analogous to the appointment obligation for public bodies appears necessary. Such an appointment obligation can be legally regulated, for example, based on the parameters of company size (measured in number of employees within the meaning of Section 26 para 8 of the German Federal Data Protection Act-BDSG) and industry and the associated criticality of data processing, provided that no blanket appointment obligation is to be introduced for companies. A more comprehensive appointment of data protection officers will help to better ensure the implementation of the requirements of the GDPR. For the specific fulfilment of tasks by data protection officers, a clarification of the task of monitoring (Art. 39 para. 1 lit. b GDPR) seems desirable in order to distinguish this term from the obvious task of control. At present, the statutory task of monitoring is often confused with a control task in

practice. According to Art. 39 GDPR, however, the data protection officer is entrusted with monitoring, which may include checking a control system in the data processing centre but is not intended to mean monitoring compliance with data protection regulations at the controller itself. In this case, the monitoring function needs to be clarified legislatively in order to emphasise this task more clearly and distinguish it from the control function.

4. fines

The much stricter sanctions regime introduced by the GDPR creates a high level of awareness of the need to ensure that personal data processing complies with the law and therefore makes a significant contribution to making the law more effective. However, there is a need for legal clarification that a notification pursuant to Art. 33 GDPR or a notification pursuant to Art. 34 para. 1 GDPR may only be used in proceedings against the party obliged to notify or the notifying party with the consent of the party obliged to notify or the notifying party. It is necessary to expressly stipulate the absolute prohibition on the use of evidence for fine proceedings for infringements under Art. 83 GDPR. This serves to safeguard the constitutional prohibition of obliging someone to self-incriminate and can be qualified as a procedural guarantee under EU law. This is the only way to resolve the tension that the controller must either accuse itself of a sanctionable data protection breach or violate the obligation to report and notify, which in turn can be sanctioned in accordance with Art. 83 para. 4 lit. a) GDPR.

5. reporting of data breaches

According to Art. 33 para. 1 sentence 1 GDPR, the notification of a personal data breach must be made within 72 hours of the controller becoming aware of the breach. In legal practice, this short notification period has proven to be very ambitious. In order to be able to carefully and conscientiously assess the facts within the company with regard to their notification obligation, an extension of the notification period - e.g. to 5 days (120 hours) - would appear to be desirable.

6. joint controllers

The legal concept of joint controllership poses an enormous challenge for legal practice. In the event of a refusal of processing on behalf pursuant to Art. 26 GDPR, joint controllership within the meaning of Art. 26 GDPR is often assumed, but this is regularly not the case. Aside from the difficulty of categorising constellations with multiple actors as joint controllership, a legal clarification would be helpful to the effect that the fulfilment of joint controllership does not constitute a legal basis for data sharing between the controllers involved. The exchange of data between several controllers requires lawfulness, which in any case does not result solely from Art. 26 GDPR. The legal consequences of joint controllership essentially include an "agreement in a transparent manner" (Art. 26 para. 1 sentence 2 GDPR) and, in principle,

joint and several liability in accordance with Art. 82 GDPR, because it refers to "any controller involved in processing" and "more than one controller", thus assuming a plurality of controllers. Due to the classification of the legal concept of joint controllership in the chapter on the general obligations of controllers and processors by the legislator, the regulation of cooperation between several controllers should teleologically focus on safeguarding the rights of data subjects. The organisational obligation should therefore contribute significantly to creating clarity for the data subject as to where and how they can exercise their rights. Joint liability, on the other hand, should be limited in its scope by the legislator to a level that is adequate for joint liability. After all, there is no transparency for each of the several controllers in the data processing of the other controllers with whom joint liability exists pursuant to Art. 26 GDPR, which makes blanket joint and several liability appear disproportionate. For this reason, liability in the sense of the "chain theory", for example, would be more in line with legal practice.

7. small and medium-sized enterprises (SMEs)

For SMEs, applying and implementing the requirements of the GDPR is generally not possible without external help. This is due in particular to the fact that the provisions of the GDPR are often interpreted and assessed as part of the evaluation of measures taken by larger companies. If these standards are then applied to all companies, they may be disproportionate to the capacities and resources of smaller companies. For SMEs, the corresponding EDPS guidelines are therefore too theoretical and difficult to implement. External help is often required in order to fulfil the requirements. An advice centre for SMEs at the data protection authorities would be helpful to raise awareness of the correct implementation of the GDPR requirements. For example, GDPR check-ups could be offered, which could benefit smaller companies in particular. Overall, the protection of personal data must be balanced with the entrepreneurial freedom of SMEs.

8 GDPR and new innovations

In the GDD's view, the technology-neutral nature of the General Data Protection Regulation can work when applied to innovative new technologies. The data protection principles are broad enough to encompass innovation-based data processing processes and to assess them flexibly. Significant interactions are expected between the AI Regulation and the GDPR in particular. Constructive best practice approaches must be created here with the support of the European Data Protection Board (EDPB).

9. conclusion

Overall, the GDPR has created important protection mechanisms for privacy, but its implementation requires continuous adaptation in order to fulfil the needs of companies and citizens alike. Greater consideration must be given to the needs of smaller companies in particular. Due to a lack of resources, many smaller companies are not in a position to implement

the requirements of the GDPR in the same way as large companies, which are regularly used as a benchmark for the development of guidelines and interpretations of the provisions of the GDPR. In many areas - particularly with regard to the rights of data subjects - it is necessary to achieve a balance between the protection of data subjects and the entrepreneurial freedom of data controllers. This can be achieved in particular by defining the requirements and limits of the individual data subject rights more clearly in order to ensure the smooth fulfilment of requests by data controllers.

Bonn, 06.02.2024

As a non-profit organisation, the Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. advocates sensible, justifiable and technically feasible data protection. Its aim is to support data processors - and data protection officers in particular - in solving and implementing the many legal, technical and organisational requirements associated with data protection and data security.

Society for Data Protection and Data Security e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de | www.gdd.de