Axel Voss

Member of the European Parliament

The new General Data Protection Regulation (GDPR)

(1) GENERAL REMARKS

The GDPR harmonizes the rules for processing personal data within the European Union. Since it is a Regulation, the new rules apply directly in all Member States. In addition, the national legislator can also introduce its own supplementary provisions for specific areas (so-called opening clauses such as in Art 88 I GDPR). Germany therefore adapted its Federal Data Protection Act (BDSG) to streamline it with the new framework. Although the GDPR already came into force in 2016, it will be applied only from 25 May 2018 due to transitional provisions granted by the EU legislator.

In accordance with Art 2 I GDPR, every natural person is protected as soon as their personal data (including name, address, place of residence, income, vehicle registration number, IP address) are automatically processed fully or partially (e.g. via PC, smartphone, camera, copier) and if this happens in a structured filing system (e.g. in a membership directory). The regulations of the GDPR apply to both one-person companies and large corporations. Also affected are all clubs, associations, parties, foundations, corporations under public law as well as federal, state and local institutions. However, the private and family life is excluded (e.g. the private correspondence of a natural person, a private address directory or the private use of social networks) but only as long as there is no commercial link (e.g. advertisement, job).

(2) THE ESSENTIAL OBLIGATIONS FOR DATA PROCESSING

Chapter 3 (Art 12 ff. GDPR) gives every natural person the right of information, access, objection and deletion. This results in the following obligations for the data processor:

- Data protection declaration (Art 12/13 GDPR): The declaration must be as simple and clear as possible, explicitly designate the responsible person as well as list the legal basis for processing personal data. It must also specify the cases in which the user's consent is required, why and for how long the respective data is stored and whether data is passed on to third parties. Finally, it must also list all rights of access and intervention of the concerned person.

- List of processing activities (Art 30 GDPR): The contact details of the data processing office, the reasons for processing, the deadlines for deletion, any transfer of data to other offices, a description of the security measures and the data protection-friendly default settings must be entered. Upon request, the list shall be submitted to the supervisory authorities. Companies, associations, etc. are only exempt from keeping a register in accordance with paragraph 5 if they employ fewer than 250 persons, the data processing is only occasional and the processing does not pose a risk to the rights and freedoms of the data subjects.

- Data protection officer (Art 37 GDPR): The person must be hired to advise on data protection obligations and to monitor and review the regulations. However, this duty only exists if the core activity of the institution is the extensive processing of sensitive data (e.g. biometric data) or if regular and systematic monitoring of the data subjects is carried out (e.g. in the case of insurance companies).

- Data protection through technology (Art 24 ff. GDPR): There is a duty to install suitable technical and organizational measures to ensure effective data protection. This means both data protection by design and data protection by default. Among other things, the data processor could pseudonymize the personal data or enable the data subject to monitor the data.

- Obligation to notify (Art 33 ff. GDPR): In the event of data protection violations that pose a risk to the rights and freedoms of the data subject, the supervisory authorities must be informed (and possibly the data subject as well) within 72 hours if possible.

- Data Protection Impact Assessment (Art 35 ff. GDPR): This procedure must be carried out if the processing is likely to present a high risk to the rights and freedoms of a natural person due to its nature / scope / circumstances / purpose. Among other things, the risks and consequences for the data subject must be assessed, a proportionality test must be carried out and effective security measures and procedures must be ensured to protect the data subject.

(3) CONCRETE CASE STUDIES

When must the data subject consent to data processing?

The consent of the person concerned must be obtained as soon as the storage, use or processing of personal data is not permitted on a legal basis (permission). Processing without consent is only possible in accordance with Art 6 I b-f GDPR: for example, if it is necessary for the performance of a contract (the data subject must be a party to the contract) or if it is necessary to safeguard the legitimate interests of the data controller (and in the latter case the interests / fundamental rights / fundamental freedoms of the data subject do not prevail). If the data is subsequently processed for a purpose other than that stated at the time of collection, a balancing of interests must be carried out in accordance with Art 6 IV GDPR.

Which formal requirements must be observed?

Under Art 4 No. 11 GDPR, consent requires a voluntary, specifically informed and unambiguous declaration by the data subject. A tacit declaration or an already ticked box in the form is not sufficient. If various data processing steps are carried out, separate consent must be obtained for each individual transaction. The data subject may revoke his/her consent at any time and without cause.

Do the declarations of consent obtained in the past still apply?

If the 'old' consent meets the requirements of the GDPR, it will continue to be valid after 25 May 2018 in accordance with recital 171 of the GDPR. Otherwise, consent must be obtained again in accordance with the new requirements.

To what extent may data processing be transferred to third parties?

As soon as a natural or legal person (e.g. an external service provider) is commissioned to process personal data, it must be ensured that the processing is carried out in accordance with the requirements of the GDPR. According to Art 5, 24 and 28 I, III GDPR, the data processor must sign a declaration of commitment, while the client must take appropriate technical protection measures.

What are the requirements for registering in an e-mail distribution list?

Only if there is already a contractual relationship the concerned person may also be registered in accordance with Art 6 I 1 f, 95 GDPR together with §7 III UWG without consent in an e-mail distribution list (e.g. for sending advertisement or a newsletter). Otherwise, the concerned person must be informed about the registration in the distribution list in accordance with Art 13 GDPR and must give his/her consent, whereby the 'double opt-in procedure' (consent to contact as well as for registration) should be selected. Due to the so-called prohibition of linking in Art 7 IV GDPR, it is prohibited to counter-finance 'free services' with the consent for an advertising use of the personal data (e.g. free newsletter for consent on other use of data).

What should be observed when using social networks?

Employee/customer or membership data may not be published in social networks without the prior consent of the person concerned. Furthermore, users must be informed about the use of social plugins on websites. Care should be taken when using platforms (e.g. for consultations, data forwarding or document exchange). It should be noted here that data transfer to other EU countries is often announced in the data protection guidelines of the respective providers. However, such data transfer is bound to certain data protection requirements and the data processor must check compliance with these rules him-/herself.

What are the special requirements for societies, clubs and associations?

The data of the members (e.g. name, address, date of birth, bank details) may be used in accordance with Art 6 I 1 f GDPR for society purposes as well as for membership support and administrational purposes as the data is then processed within the framework of a contractual relationship (= membership). However, if those matters go beyond the purposes of the society according to its statutes, the consent of the member is necessary. The use of member data for fundraising or for advertising in favour of the society is therefore permissible, as is the transfer of data to an umbrella organization (but only if the concerned person is automatically also a member there). Consent is necessary when names/postal addresses are passed on to a sponsor or other members of the association (exception: the transfer of data is the purpose of the association, for example in the case of an alumni association). The board of directors is responsible for the protection of member data.

However, if the society employs more than nine paid staff members (i.e. no volunteers), it must appoint a data protection officer, who may not be a member of the board. The data protection officer must have the necessary expertise, both in relation to the association and data law and must be committed to data secrecy.

What must be observed by societies and clubs when personal data is published?

Personal data may only be published (e.g. on the notice board) if this is in accordance with the purpose of the society, club or associations. Defamatory contents such as a ban on a member or punishments may not be published. An online publication of data must always be approved by the person concerned, unless it is specific data (e.g. team line-ups, goal scorers), which is inevitably connected to the membership. Even in this case, the person concerned can object according to Art 6 I and 21 GDPR.

(4) FURTHER ASSISTANCE

This document can only provide a first and non-binding overview of the new GDPR obligations for processing personal data and thereby makes references to the legal situation in Germany. Our office is NOT and will NOT offer any legal advice on data protection issues. For this purpose, please contact the responsible federal/state agencies, the specialists in associations or designated law firms. Further information can also be found under:

- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de
- https://www.bfdi.bund.de/DE/Home/home_node.html
- https://www.ldi.nrw.de/
- https://www.datenschutzbeauftragter-info.de/
- https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html

[released 1 June 2018]