General Data Protection Regulation (GDPR)

On 25/05/2018, the new General Data Protection Regulation (GDPR) goes into effect.

Currently, the 1995 Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data [PII (US)] and on the free movement of such data) still applies, but the technological changes of the past decades have necessitated a revision of the Data Protection Acts. The main objective of the General Data Protection Regulation is the Europe-wide uniform regulation for handling of personal data as well as adaptation to new technologies.

In order to regulate the handling of personal data uniformly, this time the EU chose the form of an official regulation. While the previous guidelines were merely enacted by the EU directive forcing member states to adapt or pass national laws, the adoption of an EU regulation is a farther-reaching step. An EU regulation not only includes catalogues of measures and guidelines for the implementation of national laws, but also automatically replaces these laws with entry into force. Regulations offer almost no leeway in terms of time and content; they are uniformly legally binding for all states immediately after entry into force and thus replace all national laws within the context of the application range.

At the same time, the GDPR contains a so-called opening clause, which allows the individual states to substantiate the rights and obligations under the GDPR by issuing individual national laws. Of course, they must be legally compliant with the provisions of the GDPR. Thus, the new Federal Data Protection Act (FDPA-new) also comes into force on 25/05/2018.

Overall, the GDPR does not contain a fundamental restructuring of the privacy policy. Rather, the already known data protection principles remain in effect and are continued by the GDPR, albeit tightened in some parts and even weakened in others.

The regulations of the GDPR are only applicable, and thus relevant, when it comes to processing of **personal data**.

According to Article 4 of the GDPR, personal data are all information relating to an identified or identifiable natural person. A natural person is considered to be identifiable if such a person can be identified, directly or indirectly, in particular by means of an identifier such as a name, identification number, location data, on-line identifier, or one or more particular features that are an expression of the identity of that natural person.

The word processing, under the terms of the GDPR means any process carried out with or without the aid of automated procedures in connection with personal data (entry, collection, organisation, ordering, storage, adaptation, modification, read-out, queries, etc.).

Personal data is thus understood as:

- Names
- Address
- Email address
- Telephone number
- Date of birth
- Account data
- License plate
- Location data
- IP addresses
- Cookies

The GDPR only draws a line where the data is actually anonymous, i.e. information that has been anonymised in such a way that the affected person can not or can no longer be identified. In such cases, it is no longer considered personal data. The privacy-related meaning of personal data will therefore most likely be expanded after the GDPR goes into effect.

The GDPR is even relevant for service providers like us, even though we are working exclusively for companies. Insofar as the processing of such data, which allows to draw conclusions about natural persons, i.e. private persons, takes place in the context of our services (directory of individual companies or partners are sole proprietorships, use of private emails for professional purposes, etc.), our services as well as our software applications are subject to all regulations of the GDPR. Even though this does not apply to all our customers and our services are generally not aimed at the processing of personal data, our solutions meet all the technical and organisational requirements for complying with the regulations of the GDPR.

In the context of the new regulation by the GDPR, the most important principles now are as follows:

1. **Prohibited unless authorised**
   This principle means that any processing of personal data is prohibited, unless it has been specifically authorised. This principle was already enshrined in the Federal Data Protection Act (FDPA), so that no new regulations are included here.

2. **Principle of purpose**
   Companies may only collect and process data for specific purposes. The purpose for collection of personal data must therefore be manageable and identifiable for both parties.

3. **Data minimisation**

   The principle of data minimisation demands that companies should collect as little data as possible. In particular, the storage of data for later use is not allowed. Again, this is not a new regulation.

4. **Transparency**

   The data processing should be comprehensible for all concerned. Even this requirement of transparency is not new, but is specified in more detail by the GDPR. In addition to the requirement of a privacy statement, each person now has additional rights. As before, companies must provide information upon request about what data they have and how they use it. In addition, every affected party now has the right to receive an overview of the data-processing activities and a list of all associated measures. This particularly includes all technical organisational measures to protect the personal data of those affected, whether against unauthorised processing or modification, against data theft or destruction.

5. **Right to be forgotten**

   Newly added by the GDPR is the right of the affected person to have his data completely deleted. The company must therefore prove at the request of the affected data subject that, if the request was made by the data subject, his data was completely deleted and is thus no longer usable.

In addition, the right to data mobility was introduced in Art. 20 of the GDPR. This gives the data subject the written right to request the transfer of his data from one processor to another processor. The respective processor must ensure this.

If a company uses the services of third parties as part of its own service provision for the affected person and if these third companies also process the personal data of the affected person, this is considered order processing. This is generally the case when using third-party software solutions that necessitate the transmission of data (for example, communications software, data hosting, etc.). As previously regulated in § 11 of the German Federal Border Guard Act (BGSG), Art. 28 of the GDPR permits such order processing only with the consent of the affected person. During order processing, the person who outsources the services to third parties must ensure that the third party complies with all data protection regulations. In this context, data transfer can only be ensured within the EU. If a data transfer of personal data takes place outside the EU, then the affected person must agree in advance for each transfer. In doing so, compliance with the statutory data protection level introduced across Europe is necessary. In this context, the US and the EU have adopted and introduced the so-called EU-US Privacy Shield. According to the EU and US Government declarations, American companies that comply with this regulation meet the necessary data protection standards and thus, in the context of order processing, also make it possible to send data to service providers in the USA and process it for third parties while processing personal data.

The new part in the context of the introduction of the GDPR is that after this regulation enters into force, not only the client but also the processor is liable for proper compliance with all data protection regulations.

In summary, it should be noted that the GDPR's entry into force will not lead to any far-reaching changes in data protection principles. Any company that processes personal data must continue to ensure that the protection of that personal data is guaranteed through technical standards and technical specifications. As part of the transparency requirement, every affected person has the right to know which third service providers are used for this process, must agree with them and must be able to see the technical and organisational measures of the processing company.

Should you have any further questions on data protection, please do not hesitate to contact us or contact our data protection officer, Attorney Christoph Najberg, at: dataprotection@uberall.com.

Best regards,

your uberall team