

# Demands on data-protection law

## Need for adjustments in the General Data Protection Regulation

In the implementation of the new regulations on data protection, situations have arisen that lead to excessive bureaucracy. Furthermore, in some places, the purpose of the new data-protection rules has been lost sight of. There is therefore a need for revision of the following points:

### Need for change in international data transfer

1. Following the CJEU ruling on the Privacy Shield agreement, there is considerable legal uncertainty among companies concerning the structures relating to the transfer of data between the EU and the USA. An **effective successor regulation** should therefore be negotiated between the EU Commission and the US authorities as soon as possible. A legally watertight and sustainable legal basis is needed for EU-US data transfer.

The current situation requires an examination by every individual company (cf. EDPB's six-step plan), which, in contrast to a central solution by the EU Commission, represents a massive amount of work. SMEs in particular do not have the necessary resources to check that the transfer of data to the USA is legally watertight. Furthermore, in the case of many services, it is impossible to reconcile the requirements of the GDPR with the legal situation in the USA (especially with regard to the access possibilities of American security authorities). If no technical alternatives are available, companies are forced into illegality.

Especially against the background of the current negotiations of the European Commission regarding an adequacy decision for the United Kingdom (and the prevailing legal powers of GCHQ there, as well as the circular exchange of intelligence information between BND, GCHQ and NSA), it is difficult to understand why data transfers to the US are subject to such high hurdles, as is the case after the CJEU ruling C-311/18 ('Schrems II').

2. The **risk-based approach** of the GDPR should also be applied to data transfers to third countries. Only such additional safeguards should be required as are proportionate to the data transferred, the scope of the processing and the likelihood and severity of risk to the data subjects.

3. The exceptions provided for in Article 49 of the GDPR should not be interpreted in a restrictive way. In particular, the GDPR allows data transfers to third countries on the basis of voluntary consent with knowledge of the risks. This is in line with the right to informational self-determination.

### Need for change in information obligations

4. Data processing that takes place at **the request of the data subject** (example: a customer hands over a business card) should be exempt from the information obligations under Articles 13, 14 of the GDPR. In this case, it is clear to the parties involved which data are processed for which purpose; no separate information is required.
5. The same applies if the purpose of the data processing is **clear** to the data subject and online services are not involved. In such cases, it should be clarified that information obligations can be limited to a minimum.
6. Data processing that becomes necessary in the course of the initiation of a contract or **for the performance of a contract** must be exempted from the strict information obligations. In such cases, it is clear to the contracting parties which data are being processed for which purpose; no separate information is required.
7. Data processing that becomes necessary for **the implementation of a membership of an association** must also be exempt from the strict information obligations. In such cases, it is clear to the members of the association which data are being processed for which purpose; no separate information is required.

### Need for change in the right of access

8. The **right to obtain information** pursuant to Article 15 of the GDPR was created in particular for the end-customer sector and for the processing of data in online transactions. In the employee sector, it causes a disproportionate amount of work in larger companies with countless automated data-processing procedures. Information in the employee sector should therefore only have to be provided if the employee him/herself has no access to his or her data. At the very least, the staff member concerned should always have to specify to which information or processing operations the request for information specifically relates.
9. It should be clarified that the right to information in the context of other legal disputes (e.g. employment-termination disputes, disciplinary warning letters, enforcement of rent increases, termination by landlords) between the contracting

parties must not be misused to undermine the **rules on the burden of proof in civil proceedings**.

10. Furthermore, it must be made clear that a **copy of the data** does not have to be submitted as soon as third-party data are included in the data sets (e.g. email correspondence, database extracts, etc.). The weighing of fundamental rights provided for in Article 15(4) of the GDPR gives rise to legal uncertainty.
11. **Internal and external communications of employees** should always be excluded from the right to information, even if no third-party data are involved (e.g. emails to functional addresses). Otherwise, thousands of emails would have to be searched and the rights of other people would be interfered with in the process.
12. Clarification is needed as to what exactly is to be covered by the "copy of the data" provided for in Article 15 of the GDPR. In particular, **internal memos and internal communications** should **NOT** be covered by the right of access.
13. It should also be clarified that **metadata in files** that are stored e.g. in Office products do not have to be provided as a copy.
14. In order to **prevent abusive requests for information**, the provision in Article 12(5) of the GDPR should be clarified to the effect that information may be refused in the event of mass requests for information to a large number of companies that give no indication of any data processing.

### Further need for change in the GDPR

15. Article 30 of the GDPR states that a **register of processing activities** only has to be kept in companies with 250 or more employees. However, such a register must always be kept when special categories of data are processed. This is the case in almost every company, no matter how small, because of church tax (religious affiliation = special category of personal data according to Article 9 (1) of the GDPR); in addition, health data (certificates of incapacity to work) are also regularly processed in small companies. The exception should therefore be deleted or differently worded, so that the register always has to be kept only in companies with 250 employees or more.
16. It needs to be clarified that a **data protection impact assessment** is not already required in the case of one-off processing of specific personal data, but only when these data-processing operations are at the core of the business purpose.

17. The obligation to conclude a contract for **processing on behalf of a controller** pursuant to Article 28 of the GDPR should not apply to data processing where the main service or a substantial part thereof is not directed at the processing of personal data.
18. In order to promote innovation and new technologies, the GDPR needs to be **more open to new technologies**. For example, with regard to AI, big data or blockchain, the processing principles of data minimization and purpose and storage limitation (Article 5(1)(b), (c), (e) of the GDPR) should be critically reviewed and concretized in a technology-adequate manner.
19. In addition to legally watertight standards for the anonymization of personal data, the processing of **pseudonymized data** should also be facilitated in accordance with the GDPR.

### Need for change in the Unfair Competition Act

20. In order to prevent the **abusive use of disciplinary warning letters**, it must be clarified in the Unfair Competition Act (UWG) that the legal requirements on data protection are not a rule of market conduct within the meaning of the UWG.

#### Contact person

**Kristina Fink**

Legal Policy Department

Telephone 089-551 78-234

Telefax 089-551 78-233

Kristina.fink@vbw-bayern.de

www.vbw-bayern.de