20 Technical and Organisational Measures (TOM)

Integrity and confidentiality belong to the key principles relating to processing of personal data. According to Article 5 para. 1 lit. f) GDPR this implies to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, which can be achieved by using appropriate technical or organisational measures. Technical and organisational measures play a role in different Articles within the GDPR, yet most importantly they have to be set up to ensure data security which is specified in Article 32 GDPR. Data security can be described as technical and organisational measures that prevent unauthorised handling of personal data. It thus serves to protect the fundamental rights of data protection and informational self-determination.

Since data protection laws first entered into force, attempts have been made to make technology subject to achieve data protection objectives. These correspond to the IT-Security objectives and are defined as availability, integrity and confidentiality. In recent years this was complemented by specifications for privacy by design. While the aim of privacy by design is to implement technical and organisational measures in the technology, technical and organisational measures that are subject to data security can be used at any time during the process of processing personal data. Technical and organisational meas-

ures that ensure data security shall prevent unauthorised handling of personal data.

Data security describes a situation in which the risk of damage to the fundamental right of protection of personal data is reduced to a minimum. Article 32 of GDPR as the central provision for data security is entitled with "Security of processing" and obliges both the controller and the processor to take appropriate measures to ensure secure processing. Article 32 GDPR substantiates the central principle of system security pursuant to Article 5 para. 1 lit. f) GDPR. Technical and organisational measures must ensure protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This includes that unauthorised persons have no access to the data and cannot use the data or the devices with which they are processed.

Pursuant to Article 32 para. 1 GDPR, controllers and processors are obliged to take appropriate technical and organisational measures to ensure a level of protection appropriate to the risk. In doing so, the state of the art, the implementation costs and the nature of the scope, circumstances and purposes of the processing as well as the different probability of occurrence and the severity of the risk for the personal rights and freedoms of natural persons must be taken into account. In its paragraph 1 the provision also entails a list, containing instruments, characteristics and procedural requirements, that can be used to ensure data security:

- the pseudonymisation and encryption of personal data (lit. a)
- the ability to secure the long-term confidentiality, integrity, availability and resilience of processing systems and services in connection with the processing of personal data (lit. b)
- the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident (lit. c)
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The GDPR follows a risk-based approach. The technical and organisational measures must always ensure a level of protection appropriate to the risk which means that the controller has to carry out a risk assessment on a case-by-case basis before each data processing operation and draw up an individually balanced protection concept.

Article 32 para. 2 GDPR specifies the risks to be taken into account when assessing the appropriate level of protection. These are, in particular, risks associated with processing, namely: unintentional or unlawful destruction, loss or alteration, unauthorised disclosure of or access to personal data. According to Article 32 para. 3 GDPR, an indication that the requirements set out in Article 32 para. 1 GDPR have been met may be compliance with an approved code

of conduct pursuant to Article 40 GDPR or a certification as set out in Article 42 GDPR.

The GDPR contains many opening clauses that allow the national legislator to enact national and subnational laws. A few of these opening clauses are set out in Article 9 para. 2 GDPR that authorises national legislators to enable processing of data concerning health and other special categories of personal data despite the fact, that processing of special categories of personal data is generally prohibited. The German Federal Data Protection Act made use of this and while it does not contain any general requirements for data security, it does contain requirements for the processing of special categories of personal data in Section 22 para. 2 BDSG. According to this Section, the following measures have to be provided in order to legally process data concerning health:

- Technical organisational measures to ensure that processing complies with the GDPR;
- Measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
- Measures to increase awareness of staff involved in processing operations;
- Designation of a data protection officer;
- Restrictions on access to personal data within the organisation of the controller and by processors;
- The pseudonymisation of personal data;
- The encryption[71] of personal data;
- Measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- Specific rules of procedure to ensure compliance with the German Federal Data Protection Act and with the GDPR in the event of transfer or processing for other purposes.

The Federal Data Protection Act (BDSG) also calls for the sensitisation of those involved in processing operations, the designation of a data protection officer and the restriction of access to personal data, as well as measures to enable subsequent verifiability of the processing operations, partly in the same spirit as and partly in addition to the measures required by the GDPR.

71 For example the BSI Guideline TR-02102 on Cryptographic procedures: Recommendations and encryption key lengths should be considered. BSI publications can be found under the following link: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

Both the provisions of the GDPR and of the German Federal Data Protection Act are rather general, which is why specific requirements cannot be derived from them. However, it is still possible to apply the annex to Section 9 BDSG sentence 1 (old version). The measures that are listed in the old version of the German Federal Data Protection Regulation can still be used to substantiate the requirements of Article 32 GDPR. Article 32 para 1 of GDPR contains a catalogue which presents "among other things" how technical and organisational measures can be designed. These include data security objectives as confidentiality, integrity and availability on the one hand and security measures to promote these objectives on the other. In contrast, the annex to Section 9 sentence 1 BDSG (old version) lists measures that are suitable for achieving data security. The term "technical and organisational measures" is to be understood broadly in the GDPR. Although it is not defined, technical and organisational measures are intended to serve very different purposes. For example to ensure fair and transparent processing of personal data within the framework of profiling or to ensure privacy by design as well as to guarantee data security.

The requirements and concepts for physical access control, electronic access control, transfer control, input control and data entry control as well as the separation requirements of the Annex to Section 9 sentence 1 BDSG (old version) can still be used under the GDPR as concrete measures to ensure the security of processing. The catalogue of Article 32 para. 1 GDPR is unstructured, random and above all not conclusive. The wording "inter alia" makes it clear that this is an exemplary list of measures, characteristics and procedural requirements that can be used to achieve the objective of data security. In addition, other measures can be used as long as they do not contradict the GDPR, but support its objectives. The security of data processing is set out as a central principle of processing in Article 5, yet the list of measures in Article 32 GDPR is rather sparse, which is why it can only be in line with the European legislator to implement further measures than those mentioned in Article 32 GDPR.

This leads to the conclusion, that the following measures (sorted by data security objectives that need to be achieved) have to be considered to assure data security—always appropriate to the risk and therefore assessed on a case-to-case basis:

- Confidentiality
  - Physical Access Control (Prevention of unauthorised access to data processing facilities)
  - Electronic Access Control (Prevention of unauthorised use of data processing and data storage systems)
  - Internal Access Control (Prevention of unauthorised copying, reading, alteration or deletion of data within the system)
  - Isolation Control (Prevention of processing data together that is collected for different purposes)
  - Pseudonymisation

- Integrity
  - Data Transfer Control (Prevention of unauthorised copying, reading, alteration or deletion of data while it is transferred)
  - Data Entry Control (Record of what and by whom is entered into a data processing system or altered or deleted)
- Availability and resilience
  - Availability control (Prevention of accidental or wilful destruction or loss of data)
  - Rapid recovery
- Procedures for regular testing, assessment and evaluation
  - Data protection management (e.g. SOP)
  - Incident response management (e.g. SOP)
  - Data protection by design and default
  - Order or contract control

This is in line with a guideline published by the German "Gesellschaft für Datenschutz und Datensicherheit e.V." (GDD), presenting and explaining necessary technical and organisational measures.[72]

For the data that is processed by the UMG which will mainly be data concerning health a high standard of data security will be necessary. However, we can not give specific advice on which technical and/or organisational measures need to be implemented as these are highly dependant on the state of the art and therefore are subject to constant change. Guidelines on these measures are published by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik—BSI).[73] Also, the data protection authorities are just beginning to pay attention to this topic.[74]

As part of the development of a data protection management system, regular reviews of the BSI publications and the publications of the data protection supervisory authorities should therefore be carried out. The effectiveness and adequacy of technical and organisational measures should be reviewed and, if necessary, adjusted as part of regular internal audits.

72 Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), GDD-Praxishilfe DS-GVO IV, Appendix; https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo.

73 For example the BSI Guideline TR-02102 on Cryptographic procedures: Recommendations and encryption key lengths should be considered. BSI publications can be found under the following link: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

74 The DSK publishes guidances which can be found at: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.