O.11 Data Protection Principles

Authors: Winfried Veil

Last update: 2021-06-25 10:12:08 | By: Winfried Veil

Created at: 2021-05-27 21:35:54

The principles for the processing of personal data are regulated in **Art. 5 GDPR**. In terms of the regulatory system, they are thus "placed in front of the brackets" of the GDPR, i.e. they apply to every processing operation.

It is quite unusual for the legislator to preface a normative text with principles in addition to objectives, scope of application and definitions. The old version of the German Federal Data Protection Act did not have such a standardisation of principles. However, data avoidance and data parsimony had already found their way into § 3a of the old Data Protection Act as "objectives" **[Tile PC.10]**. Art. 6 of the **Data Protection Directive 95/46** already contained so-called "principles relating to data quality". However, they were only addressed to the Member States, which had to observe these principles when enacting law in conformity with the Directive.

The legal significance of the "principles" is disputed. The range of possible classifications varies between

- *"programmatic of the GDPR" (Frenzel),*
- *"final programme for the processing of personal data" (Frenzel),*
- *"programme sets" (inconsequential in the result) (Schomerus),*
- *"abstract leitmotifs" (Voigt),*
- *"symbolic affirmation of Art. 16 TFEU and Art. 8 CFR" (Frenzel),*
- *"transmission belt between primary law and the further provisions of the GDPR" (Frenzel),*
- *basis of the "data protection architecture" (de Hert),*
- *"general structural principles" (Pötters),*
- *"regulations with comprehensive material content" (Buchholtz/Stentzel)*
- *"legally binding instructions for action" and "protectable legal positions" (Frenzel).*

All these classifications are based on the question of whether directly binding requirements can be derived from the principles, which would ultimately also be sanctionable and enforceable.

According to their wording, the principles of Art. 5 are binding, because they - according to the wording - "shall be" observed. However, compliance with the principles is not a prerequisite for admissibility, but "only" a prerequisite for the lawfulness of data processing. The admissibility of data processing is regulated in Art. 6, 9, 10, 22 and 44 et seq. and in subject-specific legal grounds of Union law and Member State law **[Tile O.03]**. If there is no legal ground, the data processing is unlawful. If the legal principles are not complied with, the data processing is not necessarily inadmissible (for this it depends on the severity of the infringement), but it is unlawful.

In a positive sense, the principles could also be described as "flexible". Their application is characterised by the fact that it varies depending on the processing context. In many cases of application it is not possible to clearly determine whether the requirements of the principle are met. For example, there is no clear limit at which the security of data processing can be considered "adequate". Rather, this depends on many factors (such as the purpose, context and risk of processing). Thus, the principles do not establish commandments that can simply be followed. Rather, they serve to "optimise the realisation of a desired ideal state" (*Roßnagel*).

As objective structural principles, the principles permeate all regulations of data protection law. They have a spillover effect on the interpretation of individual provisions of the GDPR. Conversely, individual regulations concretise and operationalise the principles. Further concretisations will only emerge through the legal practice of the supervisory authorities and courts.

The principles also programme the decisions of the supervisory authorities and have a blocking effect on other political programming.