22 Necessity of documents

The GDPR requires the creation and maintenance of extensive documents and directories.

- *Which documents are legally mandatory according to the GDPR (e.g. data protection concept, description of procedure, list of procedures)?*
- *Is it legally necessary to carry out a data protection impact assessment? If so, please advise us on the (document) form, scope and level of detail of this data protection impact assessment.*
- *Which documents are mandatory for DFG- or BMBF-funded research projects and what can be stored if necessary?*

The GDPR demands various documents according to the principles of accountability and transparency. Some are explicitly listed in the GDPR. Others developed in practice as usual documents of value. To the latter data protection handbooks and whitepapers belong.

The GDPR demands a directory of the processing activities as central document whose requirements are listed in detail in Article 30 GDPR. This will be the core element of the data protection documentation, which can be merged into a comprehensive compendium. This is often referred to as a data protection manual or data protection concept. Furthermore information is to be provided according to Article 13, 14 GDPR compellingly. These are summarised usually in data protection declarations (also called a privacy policies) which can be

made available in different forms to the data subject and can also be added to the data protection manual.

Further it is to be proven that consent was given. Therefore consent forms should be achieved. The wording of such declarations could also be documented in the data protection manual.

Finally a data protection impact assessment is to be made according to Article 35 GDPR and to be documented accordingly. The instrument of data protection impact assessment is a new instrument of European data protection law. Until now, information from the data protection supervisory authorities is only available to a limited extent. A "best practice" has not yet been established in this respect, but the experience gained from initial approaches should be taken into account here. The data protection impact assessment is not a one-off review but an instrument of continuous analysis and further development in the sense of a PDCA cycle.

The following minimum requirements can be derived from the legal system of Art. 35 DS-GVO:

First of all, a threshold value analysis must be carried out on an expected high risk for the rights and freedoms of a natural person that may arise from the processing of personal data. Pursuant to Art. 35 para. 7 DS-GVO, a data protection impact assessment must include at least one processing directory (shortened to reflect any high risks). Accordingly, the necessity of data processing for a specific purpose (necessity and proportionality) must be explained. The third step is to assess the risks. Finally, appropriate corrective measures should be presented.

The Datenschutzkonferenz (DSK) has provided a paper on how to perform a data protection impact assessment called "Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen", dated 26 April 2018.