18 Privacy by Design

Art. 25 GDPR demands "Privacy by Design". The trustee approach includes (cf. [Bialke, et al., 2015]):

- *informational separation of powers*
- *separation of IDAT and MDAT*
- *use of ID management according to the Master Patient Index concept for record linkage*
- *use of pseudonym management*
- *digital consent management and modular Informed Consent approach*
- *workflow-controlled TTP dispatcher approach for overarching complex TTP workflows*

Is the trustee approach presented suitable for implementing the goals of Privacy by Design?

The principle of privacy by design is introduced for the first time under EU law in Article 25 GDPR. It means that data protection is realised through or with the help of technology and organisation. The aim is to develop data protection-friendly systems that do not allow data protection regulations to be disregarded. Data protection is inherent in such systems. privacy by design thus begins in the pre-processing phase. The fundamental rights of the data subjects are already protected by draft of the system.

Article 25 para. 1 of GDPR requires the controller to take technical and organisational measures to ensure compliance with the regulation and that the rights of the data subject are protected. With regard to the timing, the provision stipulates that these measures must be taken as soon as the purposes of the processing are determined, but also at the time of the processing itself. Concerning the suitability of the measure, the following factors have to be taken into account: The state of the art and implementation costs as well as the nature, extent, circumstances and purposes of the processing. The seriousness and probability of the risks to the rights and freedoms of natural persons arising from the processing must also be taken into account. As an example of the implementation of the data protection objectives from Art. 5 GDPR—such as that of data minimisation—and thus for an effective implementation of privacy by design, the provision names pseudonymisation in accordance with Art. para. 5 GDPR.

The measures that are taken in the Trusted Third Party approach to implement privacy by design seem to fulfil the requirements set out in Article 25 para. 1 GDPR from our point of view.

As a side note we point out that some stipulations of the GDPR in our opinion do not correspond to the principle of the certainty of laws. Laws must be in any case then very specific if a national authority shall be able to sanction a possible violation of the law. In our opinion the provision is too indefinite to be subject to fines by the data protection authorities. Should there be a violation of the principle of privacy by design, the risk of a fine may be estimated as low.