2 Auditing

To document cross-system processes, audit logs are created by different systems.

To what extent may these logs contain general information (for example, nurse A created patient with pseudonym A1B2C3 in system B and stored a consent with date xx.xx.2018)?

May these logs contain personal identifying data such as "Max Müller, date of birth: 21.05.2001)?

May server logs in selected higher log levels for the development and debug process ("service case") such as DEBUG or TRACE contain IDAT for troubleshooting (i.e., log level must be set explicitly, not the normal ones)?

According to our research, there is no legal regulation that specifies in detail what a log file must look like. However, we recommend applying the general data protection principle of data minimisation and balancing it with a legitimate interest in an audit trail.

Accordingly, it would, for example, be permissible to record that a certain change was made by a certain person and, in particular, when this happened. We do not see a compelling necessity to use non-pseudonymous data.

Since personal data must also be erased in log files when a justified request for erasure is made, it is not advisable to work with clear names such as IDAT would contain.

Which data can be retained in the event of a withdrawal of a declaration of consent? What must and can be "masked" practically? Where is the line between data protection and the need for IT and information security?

Data protection and data security are characterised by partially identical objectives. These include the availability and integrity of data. If an erasure claim is justified, the right to informational self-determination prevails in case of a conflict of objectives. Limits of the erasure claim in the sense of the article 17 para. 2 GDPR (right to be forgotten) are to be found under consideration of the available technology and the implementation costs appropriate measures, also of technical kind under consideration of the available technology and the implementation costs appropriate measures, also of technical kind, in order to inform for the data processing responsible persons, who process the personal data, about the fact that a person concerned of them has demanded the erasure of all links to these personal data or of copies or replications of these personal data. In addition, claims for erasure are, inter alia, limited according to Article 17 para. 3 lit. d) GDPR where data is processed for scientific purposes and the enforcement of the claim for erasure is likely to make it impossible or seriously impede the achievement of those purposes.