ROBERT KOCH INSTITUT

Robert Koch Institute | Nordufer 20 | 13353 Berlin

VIG – Trusted Third Party for Implant Register and Health Data

Subject: Feedback on Guidelines 01/2025 on Pseudonymisation (as of 14.03.2025)

Dear European Data Protection Board,

We hereby provide feedback on Guidelines 01/2025 on Pseudonymisation (Public consultation reference: 01/2025, Start Date: 17 January 2025).

Please note that the differentiation between controller and processor is partly not clearly understandable within the text. A clarification of the roles should be included in the Glossary of the document in a similar way of what can be found at https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en.

Art. 76.-79. are problematic for dedicated trusted third parties/trust centres, because–as we understand this part of the guideline–pseudonyms like hospital case IDs/national identifiers, e.g. social security numbers, could be used to request access to the data, i.e. pseudonyms, computed by and stored at trusted third parties/trust centres.

Art. 78 is especially problematic for trusted third parties/trust centres. In the case of a dedicated trust centre (e.g. Scenario 5 in the appendix), the trust centre only stores (or cryptographically computes) the relationship between direct identifiers and pseudonyms. The trust centre does not store any other data allowing it to securely authenticate a data subject requesting his/her pseudonym, even if the data subject provides the direct identifier relating to a specific pseudonym. If for example, a trust centre stores the relationship between insurance ID numbers (the direct identifier) and pseudonyms to protect medical data in a research data centre, any third party having obtained the (unprotected/printed on documents and ID cards) insurance ID number of a data subject could claim to be this data subject and request the pseudonym in order to access the data subject's secret medical data in the research data centre. Any procedure to disclose the pseudonyms and, therefore, the relationship between a data subject and his/her pseudonym would open additional attack vectors on the secret medical information in the data centre. Therefore, a dedicated trust centre may never–under any circumstances–disclose the stored or computed pseudonyms to anybody but the controller storing the pseudonymized data.

The wording of Art. 76 should be extended by "unless otherwise regulated by state law.".

Art. 77 reads "is demonstrably unable to reverse the pseudonymisation with the assistance of another controller". As we understand it, it should instead read "[...] and is demonstrably unable to reverse the pseudonymisation withOUT the assistance of another controller.". In most cases it would be possible with the assistance of another controller and, thus, additional information to reverse a pseudonymisation–depending on the information the controller has and whether it might be lawful or not to obtain such assistance/information.

Another variation of the second approach mentioned in Art. 122-129 is one for data linkage, e.g. in Secure Processing Environments (SPE), without enabling controllers to link data themselves. This may be necessary when linking very sensitive data, e.g. health data, of independent and different kinds of controllers, e.g. state and industry-owned controllers, for research purposes: After controllers securely transmitted the identifying information or a unique identifier of a data subject and record numbers to the trusted third party/trust centre, they receive temporary transaction pseudonyms for the record numbers. Subsequently, the pseudonyms can be joined with the data records using the record numbers, which are then deleted. The controllers send their individually pseudonymized data to the SPE, which requests pseudonyms for data linkage from the trusted third party/trust centre using the transaction pseudonyms. The trusted third party/trust centre in turn uses another pseudonymisation secret of its own to compute, or randomly assigns a second-level pseudonym, which is the one to be used for linkage and use of the linked pseudonymised data. After receiving the long-term second-level pseudonym, the data records can be joined using the temporary transaction pseudonyms, which can then be deleted. The advantage of this approach is that the independent controllers do not (and cannot) know which data belong to the same data subject and that different pseudonyms are used at various stages of processing, which makes it harder to link data outside the SPE and to reverse the pseudonymising transformation without authorisation.

Please note that a definition/separation of the terms “Trusted Third Party”, “Trusted Service Provider”, and “Trust Centre” (used mostly in the Annex) should be given, or it should be stated that those are synonyms. This clarification should be included in the Glossary.

Sincerely,

Unit VIG of the Robert Koch Institute