BDI

INNONATION

STATEMENT | DATA PROTECTION | PSEUDONYMISIERUNG

# EDPB Guidelines 1/2025 on Pseudonymisation

**14 March 2025**

## Initial Remarks

BDI welcomes that the European Data Protection Board (EDPB) is specifying the requirements and framework conditions for legally compliant pseudonymisation under the GDPR, e.g. that the guidelines recognise the legitimate interest in Art. 6 (1) lit. f. GDPR as a reliable legal basis for the pseudonymisation of personal data. However, even if it is to be welcomed that the EDPB has summarised the use cases of pseudonymisation 'compactly' with these guidelines and also provides practical examples, the guidelines cannot provide significant assistance for companies. Moreover, new assessment, documentation and information obligations are mentioned in these guidelines for which the GDPR did not give any indications so far. The Guidelines do not provide detailed technical guidance on how to implement secure and efficient pseudonymisation, which are necessary, especially for SMEs. Companies need practical examples when a pseudonymisation is necessary to create compliance for the use of pseudonymized data according to Art. 6 (1) f or Art. 6 (4) GDPR.

**On (22+77): Pseudonymisation vs. Anonymisation of personal data**

The legal requirements as to when pseudonymised data is to be classified as anonymised data are being clarified during proceedings already pending before the CJEU. The GC ruled that anonymisation can be assumed if the identity characteristics are separated and it is impossible to obtain them (judgment of 26 April 2023, case no.: T-557/20). Recently, the Advocate General stated in his Opinion in Case C-413/23 P, that pseudonymised data may not be considered personal data for a third-party recipient if that recipient cannot reasonably re-identify the data subjects. One of the key factors is whether the pseudonymization is robustly secured (see N. 51 - 59 of the Opinion). So, the opinion of the Advocate General contradicts the EDPB-position that pseudonymised data remains personal data in all cases for third-party recipients. BDI therefore strongly urges the EDPB to delay any finalisation of the Guidelines until the CJEU judgment.

Dr. Michael Dose | Digitalisation and Innovation | T: +49 30 2028-1560 | m.dose@bdi.eu | www.bdi.eu

## (On 38, 51): Risk Assessment

The creation of a ‘pseudonymisation risk assessment’ is mentioned a few times in the document. Regarding the required risk assessment the guidelines should be designed in a technology-neutral way to give companies flexibility in assessing risks, while ensuring compliance with the principles of the GDPR. The risk assessment creates a new evaluation and documentation requirement that exceeds the GDPR.

## On (37): Scope of the controller's obligations

It remains unclear why the controller responsible for the pseudonymisation must also include persons in the definition of the pseudonymisation domain who are not legitimate recipients of the pseudonymised data but who could nevertheless attempt to access it.

## On (72): The requirements of multiple pseudonymisation

The requirement for the controller to modify or replace pseudonymised data again when it is passed on to third parties appears unnecessarily complex (and in some cases also unfounded). The explanatory examples do not sufficiently justify the extent to which multiple pseudonymisation is more helpful than other methods (such as data minimisation or simple pseudonymisation) in achieving the objectives of the GDPR. It shall be specified, in which cases multiple pseudonymisation is actually necessary and what specific risks has to be mitigate.

## On (77-79): Implications for the rights of the data subjects (Art. 11 GDPR)

The Guidelines only provide a brief explanation of the extent to which pseudonymization leads to an exclusion for the rights of the data subjects in accordance with Art. 11 GDPR. However, detailed explanations of the concrete conditions would be necessary. On the other hand, in the case of pseudonymization with subsequent deletion of the traceability table, data controllers are required to inform the data subjects of the additional information with which the pseudonymized data can be traced. This requirement entails additional complexity. As a result claims for access to pseudonymized data can be disproportionately prolonged, as the request, provision and review procedures become more extensive.

## On (93): Dealing with large set of personal data

Not least against the background of energy consumption and careful use of resources, it should be specified for companies how to deal with large set of personal data.

## Imprint

Federation of German Industries (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

**Transparency register number: 1771817758-48**

**Editor**
Dr. Michael Dose
Senior Manager
Digitalisation and Innovation
T: +49 30 2028-1560
m.dose@bdi.eu

BDI document number: D-2051