TaylorWessing

EDPB at a glance by Taylor Wessing

Guidelines 01/2025 on Pseudonymisation

With the guidelines adopted on 16 January 2025, the European Data Protection Board ("**EDPB**") has made **important legal clarifications** on the use of pseudonymisation. Below is a summary of these clarifications for your convenience.

1. Specification of the term "pseudonymisation"

- **Definition:** Art. 4 No. 5 GDPR defines **pseudonymisation** as **processing that** makes it impossible to attribute personal data to a specific person **without the use of additional information.** The additional information must be stored separately and must be subject to technical and organisational measures ("**TOMs**") that prevent unauthorised re-identification.
- **Application:** In certain cases, pseudonymisation of personal data is mandated by law (such as Article 66 of the European Health Data Space Regulation, Section 6 (1), Sentence 2 of the German Health Data Use Act); in others it serves as a specific **measure to implement the requirements of the GDPR** (such as the principle of data minimisation, privacy by design, TOMs).
- **Differentiation from anonymisation:** Whether pseudonymised data is still personal data depends on whether the personal reference can be restored with the means that are likely to be used according to general judgement. **This also applies when the control over pseudonymised data and the additional information required for re-identification diverge (such as separation of pseudonymised data and cryptographic key).**

2. Pseudonymising transformation

Requirements according to the Guidelines 01/2025

1. Step → **Modification and conversion of personal data**

To achieve effective pseudonymisation, identifiers must either be replaced or deleted. The choice between replacement and deletion depends on the purpose of the processing and the objectives of the pseudonymisation.

Implementation

Examples of procedures for conversion:

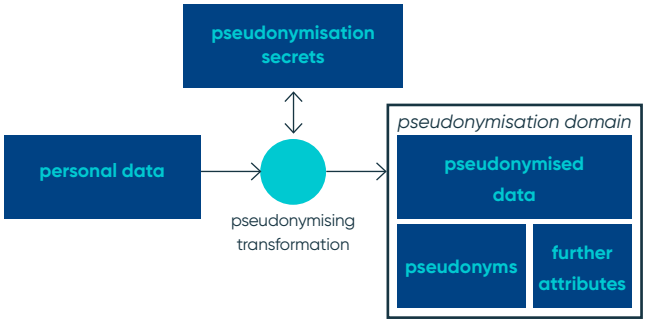
- **Cryptographic algorithms** (such as message authentication codes, encryption algorithms)
- **Procedures for creating allocation tables** (such as assigning pseudonyms to each clear dataset)

2. Step → **Separate storage of additional information for re-identification**

Additional information is generated as part of the pseudonymisation process. This includes information that is retained as part of the pseudonymisation process for the consistent pseudonymisation of different personal data relating to the same data subject, as well as information that is retained for subsequent re-identification. Examples of such additional information include cryptographic keys or allocation tables (hereinafter "**pseudonymisation secrets**").

ATTENTION: The EDPB states that additional information beyond the direct control of the controller (or processor) must also be considered when evaluating the effectiveness of pseudonymisation (such as information from social media). This applies, according to the EDPB, at least to the extent that the controller can access this additional information by appropriate means. However, the Guidelines 01/2025 leave unclear where the boundaries of accessibility of such additional information for the controller are to be drawn.

See the following diagram for the pseudonymisation procedure and the corresponding separation of pseudonymisation secrets and pseudonymised data:



3. Step

Technical and organisational measures to protect pseudonymised data

Controllers must take technical and organisational measures to prevent the unauthorised re-identification of pseudonymised data. Any unauthorised re-identification is a data breach.

Examples of common TOMs include implementing access restrictions for pseudonymisation secrets, random generation of pseudonyms and storage of pseudonymisation secrets at different locations.

3. Requirements for controllers

- **Risk identification:** Controllers must identify and precisely define the risks pseudonymisation is intended to counter. The primary objective of pseudonymisation is to mitigate these identified risks within the context of the specific processing activity. Controllers should design pseudonymisation in such a way that it effectively achieves this goal.
- **Pseudonymisation domain:** For effective pseudonymisation, the EDPB proposes a **risk-based division of data processing bodies** (and their organisational units) into those that (expectedly) only have access to pseudonymised data as a result of TOMs ("**pseudonymisation domain**") and those that have access to additional information (such as trusted third parties). The EDPB defines the term "pseudonymised environment" as one in which the controller seeks to exclude the attribution of data to natural persons (that is only pseudonymised data is available).

Our conclusion

With its guidelines, the EDPB summarises the requirements and areas of application for pseudonymisation in a compact way. This increases legal certainty for practioners and simplifies practical aspects, not least by providing criteria for the elementary risk analysis prior to the (technical) implementation of pseudonymisation. These are official recommendations issued by an authority, although they are not judicially binding. However, experience has shown that the EDPB guidelines are certainly relevant for the courts and authorities in their assessment.

Note: Questions regarding anonymisation and pseudonymisation will be addressed by the CJEU (Case C-413/23 P) with binding effect in 2025.

Contact

Stephanie Richter, LL.M., CIPP/E
+49 40 36803-0
s.richter@taylorwessing.com

Maximilian Maisch
+49 40 36803-0
m.maisch@taylorwessing.com