STIFTUNG DATENSCHUTZ

InDiCo Global GDPR & Anonymisation
18 May 2026

Standards and legal perspectives on anonymisation

Frederick Richter, LL.M.

STIFTUNG DATENSCHUTZ

Why is this topic important ?

- demarcation issues in EU data protection law / EU data law
- rising practical need for orientation

- incorrect classification of data as personal or non-personal may give rise to the risk of sanctions under both the GDPR and the Data Act

STIFTUNG DATENSCHUTZ

Anonymisation

is not regulated in the GDPR

Pseudonymisation

is regulated in the GDPR

pseudonymisation in the law

STIFTUNG DATENSCHUTZ

- **Definition** in Art. 4 No. 5 GDPR:
  - Data processing
    in which the data can no longer
    be attributed to a specific person
    without the use of additional information

- **Requirements** according to Art. 4 No. 5 GDPR:
  - allocation list has to be kept separately
  - technical/organisational measures
    have to be provided in order
    to prevent assignments or re-identifications

Importance of pseudonymisation

STIFTUNG DATENSCHUTZ

- one of the data security measures specifically named in the GDPR (Art. 32 (1)):

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Freedom to pseudonymise

STIFTUNG DATENSCHUTZ

- no formal obligation to pseudonymise data in GDPR
- derivative obligation from principle of data minimisation (Art. 5 para. 1 c)?
- derivative obligation from the principle of storage limitation (Art. 5 para. 1 e)?
  - "stored in a form which permits identification of individuals only for as long as is necessary for the purposes for which the data are processed"

Privilege through pseudonymisation

STIFTUNG DATENSCHUTZ

- Incentive: facilitation of further processing in the event of a change of purpose

  - Pseudonymisation is taken into account as a facilitating factor and orientation point in the balancing of interests when examining the compatibility of intended secondary purposes with the original purpose as a protective measure within the meaning of Art. 6 para. 4e GDPR

Importance of anonymisation

STIFTUNG DATENSCHUTZ

- with the removal of the personal reference, you completely drop out of the scope of data protection law; anonymized data is Open Data
- for anonymous data records, there are significantly more application possibilities
- data holders will only have to obey rules of the Data Act not also the GDPR stipulations

STIFTUNG DATENSCHUTZ

- **relative ("factual") concept of anonymisation**
- **anonymisation is a processing operation**
  - arg contra: definition in Art. 4 No. 2 GDPR does not mention anonymisation as a typical processing operation, but mentions erasure and destruction of data
  - arg pro: wording of Art. 4 No. 2 GDPR ("every [...] process [...] in connection with personal data")

Anonymisation in the law

STIFTUNG DATENSCHUTZ

- Art. 2 No. 7 Open Data Directive 2009:

  "Process by which documents are converted into anonymous documents that do not relate to an identified or identifiable natural person, or personal data are rendered anonymous in such a way that the data subject cannot or can no longer be identified"

relationship between deletion and anonymisation

STIFTUNG DATENSCHUTZ

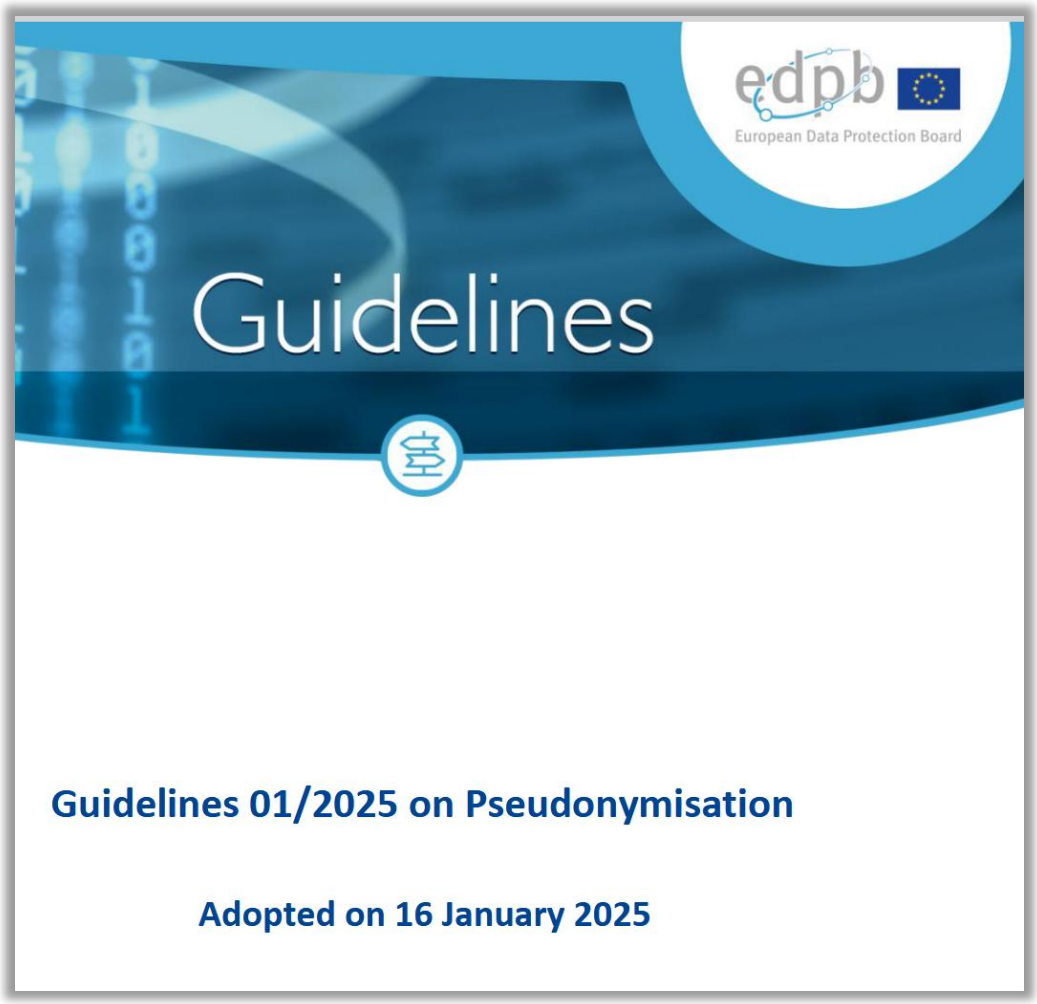
- both operations are comparable and therefore interchangeable

  - erasure is one of the options to fulfil the obligation to limit the storage of personal data under Art. 5 (1) e) GDPR
    (= to enable identification of data subjects only as long as necessary for the purpose of processing)

  - anonymisation is one of the options to fulfill an obligation to erase under Art. 17 (1) GDPR

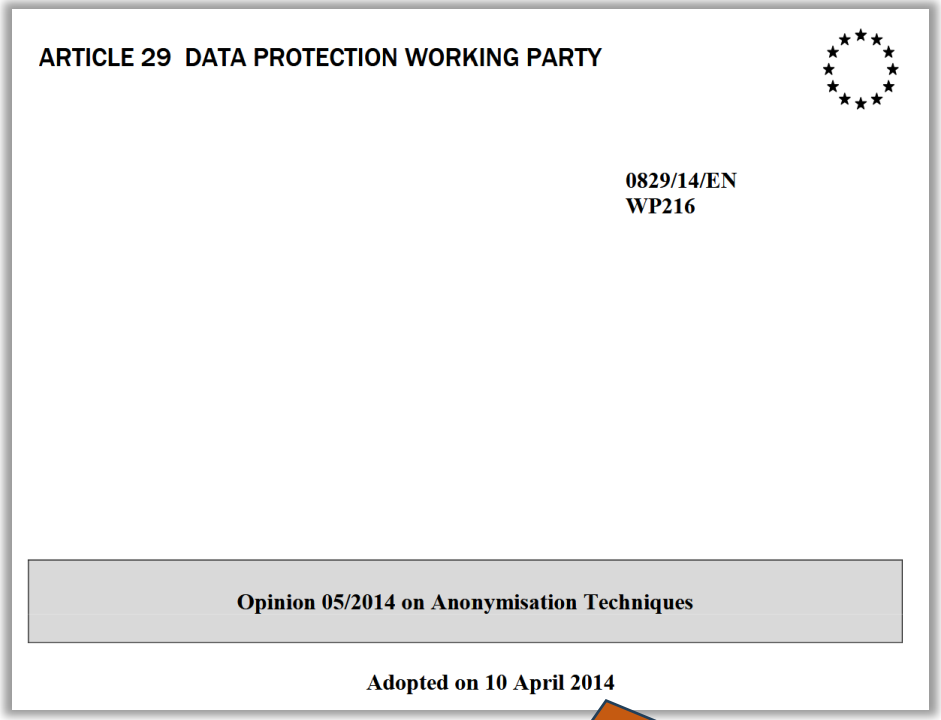
  - remaining risk of de-anonymisation
  - remaining risk of improper deletion

Public guidance needed…



Public guidance needed…

STIFTUNG DATENSCHUTZ

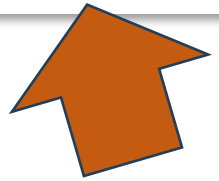


ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014



EDPB European Data Protection Board

Report on stakeholder event on anonymisation and pseudonymisation of 12 December 2025

STIFTUNG DATENSCHUTZ

- German Coalition agreement 2021:

"We promote anonymisation techniques,
create legal certainty through standards
and introduce criminal liability
for unlawful de-anonymisation."

STIFTUNG DATENSCHUTZ

- Federal Government's Data Strategy 2023:

"We will **accelerate** the **development of techniques and standards for legally compliant anonymisation and pseudonymisation.**

We are campaigning for the European Data Protection Board to present guidelines on legally compliant anonymisation."

Consequence of legal uncertainty

STIFTUNG DATENSCHUTZ

- legitimate potential uses of data are not realised
- instrument of anonymisation is used to a lesser extent due to unclear conditions
  - ➢ not in the interests of economy and research
  - ➢ not in the sense of data protection

Project of Stiftung Datenschutz

general / cross-sectoral practical **guide on anonymising data**

Approach of the practical guide

STIFTUNG DATENSCHUTZ

- focus not on absolute anonymity ("globally impossible for everyone"), our focus lies on relative anonymity (taking into account the use of available means with proportionate effort)
- Demonstration of all requirements for anonymisation from a legal and technical perspective
- Concretisation of legal requirements taking into account SME concerns
- Clarification of terminology in consideration of existing case law
- Creation of a process model, an attack model and four application classes

- Galerie

STIFTUNG DATENSCHUTZ

- 2025 Decision of the ECJ („SRB)

- court has clarified that recipients of pseudonymised data are not required to treat it as personal data provided that two conditions are met:

- recipient cannot lawfully re-identify the data

- recipient does not disclose the pseudonymised data to persons who are capable of doing so

STIFTUNG DATENSCHUTZ

- 2025 Decision of the ECJ („SRB“)

- the transmitted data was pseudonymous for the sender (= personal) but they were anonymous for the recipient

- the ability of the data transmitting entity to attribute the data is not attributable to the data receiving entity, as there was no legal/factual possibility of attribution after receipt

STIFTUNG DATENSCHUTZ

- 2025 Decision of the ECJ („SRB“)

- if the risk of re-identifying the data subject is negligible in practice (either because it is prohibited by law or because it is practically impossible due to the disproportionate time, cost and effort involved), then pseudonymised data cannot be regarded as personal data within the meaning of the GDPR in all cases and for every controller

STIFTUNG DATENSCHUTZ

- 2025 Decision of the ECJ („SRB“)

- whether a data subject is identifiable depends on the circumstances of the data processing in each individual case

- identifiability of the data subject must be assessed at the time the data is collected and from the perspective of the controller

STIFTUNG DATENSCHUTZ

= update of the case law of the ECJ ruling from 2016 ("Breyer"):

- information required to identify a person may also be held by different controllers

- however, use of the additional information must be reasonably expected - this is not the case if access is prohibited or practically impossible and therefore the risk is de facto negligible

Anonymisation in the „Digital Omnibus“ proposal

STIFTUNG DATENSCHUTZ

Amendments to Regulation (EU) 2016/679 (GDPR)

Regulation (EU) 2016/679 is amended as follows:

1. Article 4 is amended as follows:

(a) in point 1, the following sentences are added:

> ‘Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.’

Anonymisation in the „Digital Omnibus“ proposal

STIFTUNG DATENSCHUTZ

Amendments to Regulation (EU) 2016/679 (GDPR)

Regulation (EU) 2016/679 is amended as follows:

1. Article 4 is amended as follows:

(a) ~~in point 1, the following sentences are added:~~

~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~

STIFTUNG DATENSCHUTZ

Let's look forward to a bright future for anonymization !