



# POLICY BRIEF

15 09 2025

24

## PSEUDONYMIZATION

ARIANNA ROSSI



Pseudonymization	
BACKGROUND AND FIELD OF APPLICATION	<p>Pseudonymization is one of the key technical measures recognized by the GDPR for enhancing data privacy and supporting responsible data governance (see Policy Brief no. 1).</p> <p>Defined in Article 4(5), it involves <b>processing personal data in a way that prevents attribution to a specific individual without additional information</b>, which must be separately stored and protected by technical and organizational safeguards. Unlike anonymization, which irreversibly removes identifiers, pseudonymization replaces or masks them while keeping the data within the scope of the GDPR. This technique supports the principle of <b>data minimization</b> and strengthens data security and confidentiality by reducing the risks associated with unauthorized access or disclosure.</p>
HIGHLIGHTS	<p>Pseudonymization involves replacing identifiable elements in a dataset with artificial identifiers or pseudonyms, <b>reducing the direct identifiability of individuals while preserving the data's analytical value</b>, which is particularly useful in fields like medical research. The additional information that allows re-identification, such as mapping tables, must be <b>stored separately and protected through technical and organizational safeguards</b>. This is crucial when data subjects need to be re-identifiable to exercise their rights, for example.</p> <p>The process itself requires <b>careful selection of techniques based on the risk</b> to individuals' rights and freedoms, in line with data protection by design and by default.</p> <p>The European Data Protection Board<sup>1</sup> identifies two main approaches: using matching tables with randomly generated identifiers, or applying cryptographic methods such as encryption or one-way functions. In both cases, the "pseudonymization secret", whether a table or a key, must be securely protected.</p> <p>The effectiveness of pseudonymization depends on <b>what re-identification information could reasonably be accessible</b>, even beyond the data controller's control (see below). When <b>sharing pseudonymized data with third parties</b>, controllers must assess whether pseudonyms are necessary, for example, to link records or return processing results.</p> <p>The importance of this aspect has been <b>revealed in Case C-413/23<sup>2</sup></b> by the Court of Justice of the European Union (CJEU). The case concerns the Single Resolution Board (SRB), which handled the resolution of Banco Popular Español. During this process, the SRB collected comments from affected shareholders and creditors and transferred pseudonymized</p>

<sup>1</sup> European Data Protection Board, 'Guidelines 01/2025 on Pseudonymisation'

<sup>2</sup> Judgment of the Court (First Chamber) of 4 September 2025. European Data Protection Supervisor v Single Resolution Board. Case C-413/23 P.



	<p>versions of these comments to Deloitte, a consulting firm tasked with evaluating the resolution's impact. The pseudonymization involved removing direct identifiers and tagging each comment with a unique code. Crucially, only the SRB retained the key to re-identify individuals. Several individuals filed complaints with the European Data Protection Supervisor (EDPS), arguing that the SRB had failed to inform them about the data transfer to Deloitte, violating transparency obligations under Regulation 2018/1725 (the GDPR equivalent for EU institutions).</p> <p>The central issue was <b>whether the transferred pseudonymized comments constituted personal data</b> (and thus triggered GDPR obligations) <b>from the perspective of Deloitte</b>, which did not have access to the re-identification key.</p> <p>The EDPS ruled that the data were pseudonymized, not anonymous, and therefore still personal data. Since SRB retained the re-identification key, it had an obligation to inform data subjects.</p> <p>But the SRB appealed and won. The General Court<sup>3</sup> held that the identifiability of data must be assessed from the recipient's perspective (i.e., Deloitte), which <b>lacked the means to re-identify individuals. Therefore, the data were anonymous for Deloitte.</b></p> <p>In its Final Judgment (4 September 2025), the CJEU overturned the General Court's decision and clarified that personal opinions are inherently linked to individuals and qualify as personal data. Whether data are personal <b>depends on the reasonable means</b> available to the recipient to re-identify individuals. For Deloitte, the data may not be personal if appropriate technical and organizational measures prevent re-identification. For the SRB, the data remain personal, since it holds the re-identification key, thus, it must comply with GDPR obligations, including informing data subjects.</p>
<p><b>IMPACT</b></p>	<p>The ruling is crucial and implies that pseudonymized data are not automatically personal data for all parties: context matters. Transparency obligations apply at the point of data collection, especially for the controller who retains re-identification capabilities. The ruling reinforces the <b>relative nature of identifiability and the importance of assessing risk and control in data transfers.</b></p> <p>Effective pseudonymization is crucial when reusing health data (and sharing it with third parties) under the conditions set by the European Health Data Space Regulation (see Policy Brief no. 20). To uphold the principle of data minimization, the EHDS requires that <b>health data access bodies only provide pseudonymized data if data users can demonstrate that anonymized data would not suffice</b> for their intended processing purposes. In such cases, the information needed to reverse the pseudonymization process must be accessible solely to the</p>

<sup>3</sup> Judgment of the General Court of the European Union in Case T-557/20 (SRB v EDPS)



	health data access body or a trusted third party, such as a data intermediary offering confidentiality-enhancing services.
--	--