

Cybersecurity and Data Privacy Update

November 3, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

In a Landmark Decision, EU Court Clarifies When Pseudonymised Data Is Not Personal Data Under the GDPR

Executive Summary

- **What's new:** The ECJ has confirmed that pseudonymised data is not automatically “personal data” under the GDPR; its qualification depends on whether the recipient of such data can reasonably reidentify individuals, taking into account technical, organisational and legal factors.
- **Why it matters:** This decision is relevant for organisations handling, sharing or receiving pseudonymised data, as it may reduce compliance burdens and expand opportunities for data use in analytics, AI model training and service optimisation.
- **What to do next:** Organisations should review and update data-sharing practices, documentation and contracts in the light of the ECJ's decision, and continue to meet transparency obligations under the GDPR.

The Court of Justice of the European Union (ECJ) has issued a landmark decision in *European Data Protection Supervisor v Single Resolution Board* (C-413/23 P),¹ narrowing the circumstances in which pseudonymised data is considered “personal data” under the General Data Protection Regulation (GDPR).

The ECJ held in its [4 September 2025 decision](#) that pseudonymised data is not automatically personal data for all parties. Rather, its classification depends on whether the recipient can reasonably reidentify individuals, taking into account technical, organisational and legal factors.

This decision expands options for organisations handling, sharing or receiving pseudonymised data, potentially reducing compliance burdens and unlocking new opportunities for data use — particularly in analytics, artificial intelligence (AI) model training and service optimisation.

Case Background

The case arose from the 2017 resolution of Banco Popular Español, during which the Single Resolution Board (SRB), an EU agency, invited shareholders and creditors to submit comments. The SRB pseudonymised these submissions — removing names and replacing them with randomly generated codes — before transferring them to a consulting firm.

¹ Judgment of 4 September 2025, *EDPS v SRB*, C-413/23 P, ECLI:EU:C:2025:645.

In a Landmark Decision, EU Court Clarifies When Pseudonymised Data Is Not Personal Data Under the GDPR

Several participants complained to the European Data Protection Supervisor (EDPS) that they had not been informed of this data transfer, alleging a breach of transparency obligations under Regulation (EU) 2018/1725 (the GDPR-equivalent for EU institutions).

The EDPS found the SRB in violation, but the European General Court initially annulled this decision, holding that the transferred data was anonymised and thus not personal data. The EDPS appealed, leading to the ECJ's decision.

Key Findings of the ECJ Decision

- **Contextual assessment of personal data.** The ECJ stated that pseudonymised data is not automatically personal data in all contexts. Whether such data is personal depends on a contextual assessment of whether reidentification is “reasonably likely” for the recipient based on the available technical, organisational and legal measures that prevent reidentification.
- **The recipient's perspective.** The court held that the identifiability of data must be assessed from the recipient's perspective. If the recipient (*e.g.*, a consulting firm) cannot realistically reidentify individuals — due to lack of access to additional data or legal/contractual barriers — the data is not personal data in their hands and thus falls outside the GDPR's scope.
- **No “blank cheque” for pseudonymised data.** The ECJ emphasised that this is not a blanket exemption. If the recipient has, or could obtain, the means to reidentify individuals (*e.g.*, through contractual rights or access to other datasets), the data remains personal and subject to the GDPR.
- **Transparency obligations for controllers.** Even if data is pseudonymised before transfer, the original controller (here, the SRB) must still comply with the GDPR, including informing data subjects about the transfer.
- **Documenting and regularly reassessing controls.** Organisations must carefully document the technical, organisational and legal measures that prevent reidentification and regularly revisit these assessments as technology, datasets or contractual arrangements evolve.
- **Case-by-case analysis.** Organisations must conduct a careful, case-by-case analysis to determine whether pseudonymised data in their possession is truly outside the GDPR's scope. This includes reviewing technical controls, contractual provisions and the practical likelihood of reidentification.
- **Contractual and documentation best practices.** Data recipients should update data-sharing agreements and internal documentation to reflect the ECJ's revised standard, ensuring that pseudonymised data does not unintentionally fall back within the GDPR's scope.
- **Controllers' ongoing duties.** Data controllers must continue to meet GDPR transparency and information obligations regarding any onward disclosures, even when dealing with pseudonymised data.

Next Steps for Businesses

- **Review and update data-sharing practices.** Assess current and planned data-sharing arrangements involving pseudonymised data in light of the ECJ's decision.
- **Enhance documentation.** Clearly document the rationale and measures that ensure data cannot be reidentified by recipients.
- **Revisit contracts.** Update data-sharing contracts to reflect the technical and legal barriers to reidentification, and to allocate responsibilities appropriately.
- **Monitor regulatory developments.** Stay alert to further guidance from regulators and evolving best practices in pseudonymised and anonymised data.

Takeaways

The ECJ's decision provides much-needed clarity on the status of pseudonymised data under the GDPR, offering organisations a more nuanced and practical framework for data sharing and processing than the more rigid framework that GDPR regulators had adopted to date.

By emphasising the recipient's perspective and the real world likelihood of reidentification, the ruling unlocks additional opportunities for data use and innovation — as long as organisations remain diligent in their assessments, documentation and transparency.

Implications for Organisations

- **Data sharing and use.** The decision opens new opportunities for sharing and using pseudonymised data, such as in clinical trials, data licensing and AI model training, without triggering GDPR obligations — provided the recipient cannot reidentify individuals.

In a Landmark Decision, EU Court Clarifies When Pseudonymised Data Is Not Personal Data Under the GDPR

Contacts

Susanne Werry

Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

Kata Éles

Associate / Frankfurt
49.69.74220.143
kata.eles@skadden.com

Aleksander J. Aleksiev

Associate / London
44.20.7519.7000
aleksander.aleksiev@skadden.com

William E. Ridgway

Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon

Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Nicola Kerr-Shaw

Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com