Armstrong Teasdale

January 5, 2026 • Advisory • www.atllp.com

EU COURT OF JUSTICE NARROWS SCOPE OF WHEN PSEUDONYMIZED DATA IS CONSIDERED "PERSONAL DATA"

On Sept. 4, 2025, the EU Court of Justice (CJEU) issued a decision in European Data Protection Supervisor v. Single Resolution Board (EDPS v. SRB) narrowing the scenarios in which pseudonymized data is considered "personal data" under EU Regulation 2019/1725, and confirming the same rule applies under the General Data Protection Regulation (GDPR). The decision stated that pseudonymous data is not always personal data, as defined in the GDPR and the EU Regulation, but instead is only personal data if it is "reasonably likely" a data controller can re-identify the data subject. This decision will likely change how organizations handle pseudonymized data—particularly when pseudonymized data is shared in certain contexts, including AdTech, AI model training, clinical trials, and other use cases that rely on individualized but nonpersonalized data sets to detect patterns.

PEOPLE

Stewart G. Mayo, CIPP/US

F. Scott Galt, CIPP/E

Casey E. Waughn, CIPP/US

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

Artificial Intelligence

BACKGROUND

The GDPR defines personal data broadly, including both directly identifiable information (e.g., name, photo, email) and indirectly identifiable information (e.g., birthday, IP address, location). Previously, the CJEU interpreted personal data to include certain individualized identifiers such as VINs, serial numbers, and other similar identifiers when used in similar contexts that would allow the identifier to be linked back to a particular individual. Under this approach, historically, pseudonymized data (data that has been replaced with nonidentifying information—typically tokens or codes—to reduce the ability to identify the data subject) was considered personal data and therefore subject to the GDPR, when a data subject could be identified using additional information, even where the additional information enabling identification was not in the hands of the pseudonymous data holder. This was a very expansive definition of personal data, subjecting large swaths of organizations to GDPR compliance and creating controller-processor or processor-subprocessor relationships subject to GDPR compliance based solely on the sharing of pseudonymized data among organizations.

Armstrong Teasdale

EDPS V. SRB DECISION

In *EDPS v. SRB*, the CJEU held that pseudonymized data may be personal data when processed or possessed by one controller but may not be personal data when processed or possessed by another. The case stems from the collapse of a Spanish bank in 2017. The SRB, an EU agency, adopted a resolution that invited stakeholders to submit comments. The SRB subsequently pseudonymized the comments and transferred them to a consulting firm, sparking privacy-related concerns that gave rise to this litigation.

Breaking from previous guidance and interpretation, the CJEU held that pseudonymized data is only personal data when re-identification is "reasonably likely" for the ***recipient*** of the data. The CJEU noted that whether re-identification is reasonably likely depends on whether the recipient can realistically identify the data subject when considering several factors including:

- the cost of re-identification;
- the amount of time required for re-identification; and
- the available technology at the time of processing.

Accordingly, pseudonymized data is now considered personal data for GDPR purposes only when it is reasonably likely the data recipient can re-identify the data subject based on the recipient's access to additional data and their contractual and technological capabilities. Importantly, the original controller must still comply with the GDPR even if it pseudonymizes the data before transferring it because of the original controller's potential ability to relink it back to an individual as the creator of the pseudonymization. What this means in practical terms is the exact same pseudonymized data set can both be considered personal data subject to GDPR, and not be considered personal data and not subject to GDPR, depending on whether the organization is the sender (or creator of the pseudonymization) or the recipient of the data.

PRACTICAL IMPLICATIONS

Organizations now have more avenues for sharing and using pseudonymized data without being subject to the GDPR. For example, this decision opens opportunities for controllers to disclose information to recipients without the recipients becoming Article 28 processors, and subject to the requirements and data processing addendum mandates in Article 28. However, it is important to carefully assess whether it is reasonably likely the data subject may be re-identified even after pseudonymization. Organizations should review data-sharing contracts for compliance with this new standard and can craft contractual provisions to ensure re-identification is not attempted and pseudonymization or anonymization standards are satisfied.

This decision opens a multitude of data-sharing possibilities, particularly for industries that rely on individualized, but not necessarily personalized, datasets, including research and clinical trials, AI training, AdTech, research and development, and similar use cases that rely on individualized patterns, but do not necessarily concern specific data subjects.

For additional information to determine whether your organization can utilize this new decision to benefit its business practices, please contact a member of Armstrong Teasdale's Data Innovation, Privacy, and Security team or your regular Armstrong Teasdale attorney for guidance.

Armstrong Teasdale's Data Innovation, Security, and Privacy team will continue to monitor and provide updates regarding this and other GDPR developments.