Data Protection – New Approach by the CJEU on the Transfer of Pseudonymized Data *(EDPS v. SRB, Case C-413/23 P*)

by Raluca Bădilă, Avocat (Attorney at Law RO)

On 4 September 2025, he Court of Justice of the European Union (CJEU) issued a practically relevant ruling that provides clarity on the handling of pseudonymized personal data under the EU General Data Protection Regulation (**GDPR**).

Pseudonymization is defined in the GDPR as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

Background of the Case

Following the resolution of a Spanish bank, the competent authority (Single Resolution Board – SRB) made a preliminary decision on whether it was necessary to compensate the former shareholders and creditors of the bank.

To this end, a procedure was organized to allow those affected to submit comments on the preliminary decision. Some of these comments were transmitted to an auditing firm in pseudonymized form.

A number of affected shareholders and creditors filed a complaint with the European Data Protection Supervisor (EDPS), claiming they had not been informed about the disclosure of their data to the auditor.

The EDPS found that the auditor in this case was indeed a recipient of the complainants' personal data. Moreover, it concluded that the SRB had violated the information obligations set out in the GDPR.

The SRB then brought an action for annulment of the EDPS decision. The General Court partially upheld the action and annulled the contested decision (**Case T-557/20, SRB v. EDPS**).

The EDPS appealed this ruling to the Court of Justice of the European Union (CJEU).

Decision and Reasoning

The appeal focused on three key legal questions:

- Does a person's opinions constitute personal data?
- Under what circumstances can pseudonymized data be considered personal data?
- Does the data controller have an obligation to inform individuals when transferring pseudonymized data?

The CJEU first held that the information in the comments transmitted to the auditor was "closely linked to the persons" who submitted them, expressed the personal views or positions of their authors, and as such, **constituted personal data**.

The Court further ruled that **pseudonymized data are not always and for every party to be considered personal data**. This means the classification depends on the specific circumstances

of the case and requires assessing whether the recipient has “reasonable means” – technical, legal, or otherwise – to identify the individuals concerned. If such a risk is “nonexistent or negligible,” pseudonymized data does not fall under the definition of personal data.

Finally, the CJEU ruled that the identifiability of the data subject must be **assessed at the time the data are collected and from the perspective of the data controller** (in this case, the SRB). The controller’s transparency obligation to inform the data subjects applies prior to the data transfer – regardless of whether, from the recipient’s point of view (after pseudonymization), the data still constitutes personal data.

In other words: for the disclosing controller, pseudonymized data remains personal data as long as they retain access to the means to re-identify the data subject. Therefore, under Article 13(1)(e) GDPR, the controller must inform data subjects about the transfer of their pseudonymized data to third parties, even if such data is anonymous for the recipient.

Conclusion

This ruling is highly significant for data protection. It states or reaffirms, among other things, the following:

- Data controllers must generally inform affected individuals about the recipient(s) of their personal data prior to disclosure.
- Pseudonymization does not automatically deprive data of its personal character.
- What matters is whether the data subject is identifiable from the perspective of the controller: if the controller can still identify the person from the data, the transparency obligation remains – even if the recipient cannot identify the person.
- This also affects the liability of recipients towards the data subjects.

Contact and further information:

STALFORT Legal. Tax. Audit.
Bucharest – Bistrița – Sibiu

Office Bucharest:
T.: +40 – 21 – 301 03 53
F: +40 – 21 – 315 78 36
M: bukarest@stalfort.ro
www.stalfort.ro