EDPB European Data Protection Board

Stakeholder event on anonymisation and pseudonymisation in light of the EDPS v SRB judgment - discussion paper

European Data Protection Board

1 Previous work of the Article 29 Working Party and the EDPB

The Article 29 Working Party Opinion 4/2007 on the concept of personal data provided guidance on how the concept of personal data in Directive 95/46/EC should be understood by clarifying when information relates to a natural person and when that natural person can be considered to be identified or identifiable. The Working Party extended this work in its Opinion 05/2014 on "Anonymisation Techniques".

The EDPB has been working on a new set of guidelines on anonymisation and pseudonymisation under the GDPR. As the first result of this effort, on 16 January 2025 the EDPB published the Guidelines 01/2025 on Pseudonymisation and held a public consultation on its contents. The work on the Guidelines on Anonymisation is still in progress. Already, the Joint Guidelines on the Interplay between the Digital Markets Act (DMA) and the GDPR contain valuable guidance on achieving anonymity in the context of the transmission of gatekeeper data pursuant to Article 6(11) DMA.[1]

In light of the judgment in Case C-413/23 P, *EDPS v SRB*[2], and to ensure that it can provide concise, practical and clear guidance, the EDPB is now reassessing its work made so far in order to take into account the latest case law of the Court of Justice of the EU.

2 The *EDPS v SRB* judgment

On 4 September 2025, in its judgment in Case C-413/23 P, *EDPS v SRB* the Court of Justice set aside the judgment of the General Court of 26 April 2023 in T-557/20 *SRB v EDPS*. A summary of the facts can be found in the press release from the Court.

First, the Court found that the EDPS was entitled to conclude that comments transmitted to Deloitte constituted information relating to natural persons, namely the authors of those comments.

Secondly, the Court clarified two points:

- Pseudonymised data do not constitute, in all cases and for every person, personal data. Pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.[3]

[1] See, in particular, paragraphs 179–181.
[2] C-413/23 P *European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB)* ("*EDPS v SRB* judgment").
[3] *Ibid*, paragraph 86.

- In [other] circumstances, the fact that the information enabling the data subject to be identified was in the hands of other people did not actually prevent that subject from being identified in such a way that the subject was not identifiable for the controller.[4] In particular in the context of a potential subsequent transmission of data to third parties, and in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transmission and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.[5] This applies both to the receiving and the transmitting party.

The Court further confirmed that the relevant perspective for assessing whether the data subject is identifiable depends, in essence, on the circumstances of the processing of the data in each individual case[6]. When assessing the obligation to provide information where personal data are collected from the data subject, the relevant perspective for that assessment is that of the controller at the time of collection[7]. When assessing the personal nature of data published through a press release, the relevant perspective is that of the recipients.[8] Notably, while this relevant perspective was established explicitly in the *EDPS v SRB* case, previous decisions appear to have instead addressed this question implicitly.[9]

When assessing whether data is personal, all the means reasonably likely to be used by the controller or any other persons must be considered. The Court clarified that the reference to 'any other persons' refers to persons "who have or may have access to the means reasonably likely to be used for the purposes of identifying the data subject"[10], which includes having means reasonably likely to be used allowing access to the data in question.

Finally, the Court ruled that, in the context of the right to information under Regulation 2018/1725, Article 15, the identifiable nature of the data subject must be assessed from the perspective of the controller who collected the data (in this case, the SRB). It was not disputed between the parties that the SRB, as controller, had all the information necessary to identify the authors of those comments. Consequentially, the Court found that the information at issue constituted personal data for the SRB.[11]

---

[4] *Ibid*, paragraph 83.
[5] *Ibid*, paragraph 85.
[6] *Ibid*, paragraph 100.
[7] *Ibid*, paragraph 111.
[8] C-479/22 P *OC v European Commission*, paragraphs 52–64 and *EDPS v SRB* judgment, paragraph 81.
[9] C-479/22 P *OC v European Commission*, paragraph 64; C-319/22 *Gesamtverband Autoteile-Handel v Scania,* paragraphs 49–50; C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit*, paragraph 49; and C-582/14 *Breyer v Bundesrepublik Deutschland*, paragraphs 47–48.
[10] *EDPS vs SRB* judgment, paragraph 87.
[11] *EDPS v SRB* judgment, paragraph 120.

3 Questions to stakeholders

Question 1: According to the Court, the relevant perspective for assessing identifiability depends, in essence, on the circumstances of each individual case[12]. Based on your experience, what are the use cases where further guidance could be beneficial regarding the contextual assessment of the relevant perspective(s)? Further, are there any specific GDPR provisions which pose particular challenges for this assessment? For example, what open questions remain in practice considering different roles in processing, e.g. controller-processor relationship, joint controllership?

Question 2: According to the case law[13], a controller may need to assess the means of identification available through a transmission of the data in question to third parties. In relation to this, the data could possibly change its nature (e.g. data considered anonymous could become personal) due to (potential) transmissions between different parties, which may also have consequences for the initial controller. Which types of use cases (e.g. connected with third country transfers, publication to the general public) present practical challenges to ascertain the presence or absence of means of indirect identification? Which kind of measures could controllers take to recognise the presence of such means?

Question 3: The Court emphasised the restriction of the analysis to means reasonably likely to be used by the controller or another person[14]. Circumstances determine which means are 'reasonably likely' to be used. What kind of measures can a controller implement to limit the means 'reasonably likely' to be used? How can this be done in the case of subsequent transmissions by intended recipients to third parties who may be able to identify the data subject?

Question 4: In your experience, in which use cases would a controller processing data that has undergone pseudonymisation (pseudonymised data) have problems in deciding whether they are personal for a given recipient? What would be technical and organisational means that the pseudonymising controller could apply and that a recipient could not lift?[15]

[12] *EDPS v SRB* judgment, paragraphs 100–111.
[13] C-319/22 *Gesamtverband Autoteile-Handel v Scania*, paragraph 49; *EDPS v SRB* judgment, paragraphs 84–85.
[14] *EDPS v SRB* judgment, paragraphs 79–85.
[15] *EDPS v SRB* judgment, paragraph 77.