Author:

Dr. Ulrich Baumgartner
LL.M. (King's College London), CIPP/E | Partner

19.09.2025

The SRB-Ruling of the European Court of Justice – What It Means in Practice (also for the Data Act)

Authors: Dr. Ulrich Baumgartner | Prof Dr. Boris Paal

In short:

The CJEU's judgment in the SRB case (Case C-413/23 P) makes fundamental statements about the definition of personal data and therefore the scope of EU data protection law. In this newsletter, we focus on what the ruling means for future practice beyond the specifics of the actual case.

Most importantly, the CJEU continues its established "relative approach" regarding the concept of personal data. The Court has repeatedly taken a person- and context-relative understanding of personal data, starting with its Breyer ruling of 2016 (C-582/14), followed by several other rulings since then (think of the cases Nowak (C-434/16), IAB Europe (C-604/22), Scania (C-319/22), OLAF (C-479/22 P) etc.). Therefore, it is neither new nor surprising that the CJEU again follows a relative approach also in the SRB case. What is new, however, is that the court finally found very clear words against the overbroad "absolute" approach

taken by the EDPS in the SRB case – and by most German and EU data protection supervisory authorities for decades. Therefore, the SRB ruling provides greater clarity than previous CJEU case law.

Unfortunately, the judgment also contains some less clear statements by the Court which will lead to new legal uncertainty.

The decision was not rendered through the usual preliminary ruling proceedings (Art. 267 TFEU), but via an appellate procedure under Art. 256 TFEU concerning the GDPR's "sister" Regulation 2018/1725 addressed to EU institutions. However, the CJEU explicitly stated that its findings equally apply corresponding GDPR provisions.

1. What the Court Said

First, the CJEU again rejects the "absolute" notion of personal data favored by many data protection authorities, holding instead that data is only personal for a recipient if that entity can realistically identify individuals, considering available knowledge and contextual risks.

Consequently, pseudonymized as defined in Art. 4(5) GDPR does not always qualify as personal data (as put forward by the EDPS in this case). Rather, pseudonymized data may not be personal for a recipient (in the present case Deloitte) without access to the additional information required for identification, even though the controller (in the present case SRB) retains that capability. In other words, the same set of pseudonymized data might be personal data for one party but not for another party.

Therefore, the Court requires a case-by-case analysis whether the individual party processing the data has access to additional knowledge reasonably allowing it to attribute the data to an identifiable natural person.
In this context, and with reference to the CJEU's OLAF decision of 2024, the ruling emphasizes a risk-based approach: If the risk of (re)identification is negligible for an individual party (e.g., because it would require disproportionate effort), the data is not considered personal data for that party.

Secondly, the Court introduces a nuanced "perspective-based" approach where multiple parties process personal data (e.g., in a controller – processor relationship)– in which case it must be determined which party's perspective is decisive to make it subject to GDPR obligations (like the information obligations addressed by the court).

Thirdly, the CJEU reiterates the concept of "indirect identifiability" which it first mentioned in the Scania case. Unfortunately, also in the SRB case, the Court does not further elaborate on this concept – and as a result creates new legal uncertainty. For the second time since his Scania decision, the Court mentions this concept in relation to a scenario where a party passes on information that is not personally identifiable for such party to a data recipient who, for his part, can establish personal references on the basis of additional knowledge. In this case and limited to the transfer as such, the Court seems to attribute the recipient's additional knowledge to the transferring party without further examination – with the result that the data becomes personal also for the transferring party with regard to the transfer.

Finally, it is also important what the Court did not say: The decision is silent on when a risk of identification is "negligible" and which party bears the burden of proof for demonstrating the absence of personal data.

2. What the Ruling Means for Future Practice

First and foremost, the ruling means that data protection supervisory authorities have to radically change their approach as to what constitutes personal data. They can no longer apply their overbroad view that every information is personal data “in all cases and for every person” only because there might be someone else who holds the additional knowledge for identification.

This applies in particular to the supervisory authorities' understanding of pseudonymization which the Court has thrown out. The ruling therefore also renders the EDPB Guidelines 01/2025 on Pseudonymization obsolete.

However, the CJEU ruling has wider implications well beyond the processing of pseudonymized data. In practice, any sanctions or activities of data protection supervisory authorities further disregarding the relative concept of personal data are now legally contestable with high chances of success. This opens up new options for defense against regulator sanctions.
Equally important, anonymization is now much easier to achieve, as the CJEU (again) made clear that a risk-based analysis is required. This means that data can be anonymous although there remains a (negligible) risk of (re-) identification.

However, the required case-by-case analysis of whether personal data is processed might be complex, in particular where multiple parties process the same data (e.g., in a controller-processor or in a controller-to-controller scenario).

Finally, the concept of “indirect identifiability” is particularly relevant under the EU Data Act for data holders when dealing with data access claims. Data holders will have to check whether users or data recipients can identify data subjects – in which case the granting of access to data would require a GDPR legal basis for the data holder even if the data holder is unable to identify the data subjects.
There follow a number of other highly-relevant questions from the ruling, e.g., is a data processing agreement or are SCCs required if the “processor” cannot identify data subjects?

3. What Companies Should Do Now

- Take a fresh look at your internal GDPR documentation to see whether really everything you classified as personal data meets the CJEU test. Likely there is fewer personal data than expected.
- Make use of the CJEU ruling when dealing with the EU Data Act. The relative approach to personal data makes life easier, but data holders should carefully consider the CJEU's concept of "indirect identifiability" before making data accessible to users and data recipients.
- Take advantage of the new options for defense if you are dealing with a supervisory authority or data subject complaints or damage claims.
- Revisit the benefits of anonymization – the ruling offers new options whenever identifiers are used instead of "clear data". This is important news for research projects, online tracking and many other scenarios.

Stay tuned for further newsletters with more details on what the ruling means in practice! In our next newsletter, we will address the need for data processing agreements or SCCs in a controller-processor relationship if the latter cannot identify.