

## Between Nuance and Caution: How to Read the CJEU in EDPS v SRB

Stalla-Bourdillon, Sophie

*Published in:*  
Privacy and Data Protection

*Publication date:*  
2025

*License:*  
CC BY-NC-SA

[Link to publication](#)

*Citation for published version (APA):*  
Stalla-Bourdillon, S. (2025). Between Nuance and Caution: How to Read the CJEU in EDPS v SRB. *Privacy and Data Protection*, 26(1), 6-10.

### Copyright

No part of this publication may be reproduced or transmitted in any form, without the prior written permission of the author(s) or other rights holders to whom publication rights have been transferred, unless permitted by a license attached to the publication (a Creative Commons license or other), or unless exceptions to copyright law apply.

### Take down policy

If you believe that this document infringes your copyright or other rights, please contact [openaccess@vub.be](mailto:openaccess@vub.be), with details of the nature of the infringement. We will investigate the claim and if justified, we will take the appropriate steps.

# Between nuance and caution: how to read the CJEU's judgment in EDPS v SRB

---

**Sophie Stalla-Bourdillon,**  
Co-Director at Brussels Privacy Hub, unpacks the CJEU's approach to anonymisation in the EDPS v SRB case

---

**O**n 4th September 2025, the Court of Justice of the European Union ('CJEU') delivered a landmark judgment in [EDPS v SRB \(Case C-413/23 P\)](#) in which the CJEU clarified the notion of personal data in the context of transmitting pseudonymised data to third parties — an issue it had not previously addressed, at least in these terms.

Finding that the General Court had erred in law on several points, the CJEU examined two constitutive elements of the legal definition of personal data as set out in the opinion of the European Data Protection Board ('EDPB')'s predecessor on the concept of personal data: the 'relating to' criterion and the 'identifiability' criterion.

In line with the Opinion of the Advocate General, the CJEU drew a clear distinction between these two elements. More specifically, with respect to 'identifiability', the CJEU disagreed with the European Data Protection Supervisor ('EDPS') and confirmed that pseudonymisation may result in anonymisation, and thereby may affect the legal status of the data once the context of the entity holding the data is taken into account.

Although the CJEU adopted what is sometimes described as a relative approach to anonymisation (with several variations of this approach existing), it held that information about recipients is essential for data subjects to exercise their rights. The obligation to provide this information therefore arises at the moment of collection, where the controller conducting the anonymisation process holds personal data.

The CJEU judgment appears to provide a foundation for the emergence of a uniform approach to anonymisation. Yet, two critical pitfalls must be avoided.

**1. Formulating a test that disregards established de-identification techniques and statistical disclosure control methods:** Although the 'means' test for identifiability is grounded in a standard of reasonableness, it is important not to undermine the framework by reducing it to a casuistry based merely on subjective judgment calls.

**2. Adopting a formalistic definition of personal data that downplays the impact of singling out in potentially harmful contexts, such as profiling or taking action in relation to individuals:** Identifiability rests on two factors: whether individuals can be distinguished from one another (distinguishability), and whether additional identifying information is accessible that could then be associated with person-level data and reveal their identity (accessibility). Because assessing accessibility often relies on threat modelling assumptions, given the difficulty of precisely mapping the information a situationally relevant attacker might possess, it is more appropriate to focus on distinguishability only when the potential for harm to data subjects is significant.

With these pitfalls in mind, the CJEU judgment should be read carefully to understand how far its reasoning really goes. This commentary therefore unpacks the CJEU's approach and highlights three main takeaways.

## Background to the case

On 7th June 2017, the Single Resolution Board ('SRB') had adopted a decision to place a Spanish Bank (Banco Popular) under resolution, and the resolution scheme was subsequently endorsed by the European Commission. Following the resolution of Banco Popular, the SRB asked the company Deloitte to undertake a valuation of difference in treatment to determine whether the shareholders and creditors of Banco Popular would have received better treatment if the bank had entered into normal insolvency proceedings. A week later, Deloitte sent that valuation to the SRB.

A couple of months later, the SRB published on its website a notice regarding its preliminary decision about compensation for former shareholders and creditors and then launched the right to be heard process, which comprised two phases: registration and consultation.

During the registration phase, the affected shareholders and creditors were invited to express their interest in exercising their right to be heard using an online registration form. The form

included proof of identity and ownership of written down or converted and transferred capital instruments of Banco Popular. This information was accessible to a limited number of SRB staff, i.e., those tasked with processing those data in order to determine eligibility for compensation.

During the consultation phase, comments were processed. The members of SRB staff responsible for processing the comments did not have access to either the data collected during the registration phase, which was separated from the comments, nor to additional information that would make it possible to trace back the identity of the affected shareholder or creditor from the unique alphanumeric code assigned to each individual comment submitted via the form. The alphanumeric code was a 33-character unique reference that was randomly created when the form responses were received.

During the consultation phase, comments were filtered, categorised and generalised to eliminate duplicates. Deloitte was unaware whether a comment had been made by one or more participants. Deloitte had not been given the means to link the comments to the identifying data; it did not have access to the data collected during the registration phase. The alphanumeric codes had been used for audit purposes to verify, and if necessary to demonstrate, in legal proceedings, that each comment had been taken into consideration.

Shareholders and creditors filed complaints with the EDPS, alleging that the SRB had failed to inform them of

data transfers to Deloitte through its privacy statement.

The EDPS found Deloitte, as recipient of the pseudonymised data, to be a recipient of personal data, and ruled

that SRB had violated Article 15(1) (d) of Regulation 2018/1725, i.e., the data protection regulation for EU institutions ('EUDPR'). The General Court annulled the EDPS decision in part. The EDPS appealed.

The EDPS, with whom the EDPB agreed, raised two grounds of appeal: infringement of Article 3(1) and (6) EUDPR and infringement of Article 4(2) and Article 26(1) EUDPR.

### The CJEU's reasoning

The CJEU concentrated its analysis on the first ground for appeal. It held that the General Court had committed several errors of law but did not fully endorse the reasoning advanced by the EDPS. In fact, the CJEU departed from the EDPS on one important point, as explained below.

The CJEU reiterated that the definition of the concept of 'personal data' set out in Article 3(1) of EUDPR is essentially identical to that in Article 4(1) of the GDPR, which itself is essentially identical to that set out in Article 2(a) of the Data Protection Directive 95/46/EC.

The CJEU acknowledged that the concept of personal data comprises two important and distinct building blocks: the data must 'relate to' a natural person and the natural person must be identified or identifiable.

**'Relating to':** As regards the 'relating to' criterion, the CJEU, referring to the Nowak judgment ([Peter Nowak v Data Protection Commissioner, Case C-434/16](#)), articulated a two-prong test. To understand this aspect of the judgment, it is useful to refer to the Advocate General's Opinion, which stated that either the data are presumed to be relating to an individual or they are not, and the content, purpose or effects of the data must then be examined. According to the Advocate General, "it could be presumed (...) that an opinion or assessment necessarily relates to its author". On this basis, it followed that the General Court thus erred in holding that the EDPS had to assess the content, purpose or effects of those comments, since "it was common ground that [the comments] expressed the personal opinion or view of their authors".

**'Identified or identifiable':** The CJEU's finding as regards identifiability is significant. First, the CJEU noted that pseudonymised data are not mentioned in the legislative definition of the concept of 'personal data' in Article 3(1) EUDPR, but that their characteristics are apparent from Article 3(6) EUDPR. Second, as stated in the Opinion of the Advocate General, for Recital 16 EUDPR to have any practical effect, pseudonymised data will not always constitute personal data.

Third, although pseudonymisation is first and foremost a set of "technical and organisational measures to reduce the risk of a data set being correlated with the identity of data subjects", pseudonymisation may have an impact on whether or not those data are personal within the meaning of Article 3(1) EUDPR because the objective of pseudonymisation "is, among other things, to prevent the data subject from being identified solely by means of pseudonymised data."

—  
**"The CJEU's finding as regards identifiability is significant. First, the CJEU noted that pseudonymised data are not mentioned in the legislative definition of the concept of 'personal data' in Article 3(1) EUDPR, but that their characteristics are apparent from Article 3(6) EUDPR. Second, as stated in the Opinion of the Advocate General, for Recital 16 EUDPR to have any practical effect, pseudonymised data will not always constitute personal data."**  
 —

*(Continued from page 7)*

On this point, it is important to stress that the CJEU's reasoning remains nuanced and goes two ways. Just like pseudonymisation does not always make data remain personal, the existence of additional information implies that pseudonymisation does not always lead to anonymisation.

Rejecting the EDPS' interpretation, the CJEU found that in the hands of the third party, the pseudonymised data "may have the effect that, for that company, those comments are not personal in nature". Two conditions must be met for arguing that the third party does not hold personal data. First, one must establish that the third party is not in a position to lift the technical and organisational measures applied on the data and its environment. Second, those measures must be effective (even if not lifted): those measures must "in fact be such as to prevent [the third party] from attributing [the data] to the data subject including by recourse to other means of identification such as cross-checking with other factors".

Importantly, a contextual assessment is needed to determine whether the third party receiving the data can be deemed not to be in a position to identify the data subjects: access to both the additional information segregated by the controller and other types of accessible additional information, e.g., publicly available additional information, are in scope for the analysis.

Further, it is not enough to allege that the third party holds anonymised data because the data has been pseudonymised by the controller. "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 transfer and any subsequent processing of those data by those third parties", stated the CJEU. It would thus seem that it is for the party claiming the anonymisation status to establish that it is reasonable to rule out re-identification capabilities.

While a contextual analysis appears conceptually sound, the CJEU did not push the reasoning further. It did not explain in what respects the anonymisation standard imposes more stringent requirements than the standard under Article 12 EUDPR (equivalent to Article 11 GDPR) for example, which presupposes a party-specific assessment and rests on the assumption that the data holder is not in a position to re-identify the data subjects. Logically, the difference should lie in the fact that for an Article 12 EUDPR claim, no systematic demonstration about re-identification risks is needed.

The contextual assessment as formulated by the CJEU appears to require refinement, as it seems to focus upon access to data by the anticipated recipient only. Depending upon the release model adopted by the controller, the recipient of the data deemed to be anonymised may have to put in place appropriate security measures to prevent access by unauthorised actors (i.e. unanticipated recipients), to claim that re-identification risks have been mitigated to an acceptable level. This aspect of the question was not considered by the CJEU.

While the CJEU rejected an interpretation of Recital 16 that would imply that a natural person identifiable in the hands of the controller must automatically be regarded as identifiable in the hands of third parties, it did not suggest that the situation of the controller must always be segregated from that of the data recipient for the purpose of the analysis. The CJEU clarified 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". Accordingly, one could try to argue that the data continued to constitute personal data in the hands of Deloitte.

One point added by the EDPS was that Deloitte should be considered a processor and as such its situation should not be segregated from that of the controller for the purposes of the analysis. The UK Information Commissioner's Office ('ICO'), draws a distinction between recipients acting as processors and joint controllers

and others. In its recent guidance on anonymisation, one finds the following recommendation: "You should note that the 'whose hands' approach only applies when disclosing information to an organisation who is not acting with you as a joint controller or as your processor". The CJEU refused to examine this argument, as this was not necessary to uphold the appeal.

Finally, the CJEU confirmed the connection between the concept of reasonably likely means with that of reidentification risk, and stated that "a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant".

**Obligation to inform about recipients:** Ultimately, the CJEU recognised that the identity of the recipient is a significant factor in assessing the robustness of the anonymisation process. Although it is not clearly stated by the CJEU, the quality of the data security measures implemented by the recipient may be relevant in evaluating the effectiveness of anonymisation. Consequently, the obligation to inform data subjects at the stage of collection is to be welcomed.

It should not be unduly difficult to provide clarity regarding both the modalities adopted for the anonymisation process, including the release model, and the upshot that, once transferred, the recipient will treat the data as anonymised. It is worth noting that there is a general push for greater transparency in the use of anonymisation techniques given that data security, just like system security, should not depend upon secrecy. In addition, a one-to-many release model has different implications than a one-to-a few or a one-to-one. Being precise about who the recipients are is, therefore, important.

The CJEU stressed the importance of quality information when the legal basis of the processing is consent, but also used broader language and refers to the importance of quality information for exercising data subject rights.

Such a transparency obligation should not be contingent solely on the legal basis of consent, and there should be ways to explain in simple terms what is happening to the data.

Anonymisation triggers transparency and accountability obligations, as emphasised by the ICO, which writes that “You must explain your approach to anonymisation as clearly as possible in your privacy notice, including any consequences it may have [and you must make the policy clear and easily accessible”.

It might be useful to consider sharing as made of two stages: making available and access. Such a framing might help explain the consequences of the CJEU’s solution.

For example, if there is no access to personal data because data are anonymised for the receiving end, there is no restricted international transfer although data remains personal on the delivering end. With this said, even if the data are deemed anonymised on the receiving end, it is likely that contractual obligations will be needed to impose technical and organisational measures on the receiving end (e.g., access control, purpose limitation) and thereby achieve anonymisation at the receiving end. In any case, it is important to make sure the threat model is adapted to the international context, which might change modelling assumptions as regards the prior knowledge of potential attackers.

## Main takeaways

**1. This judgment is nuanced:** It would be risky and inappropriate at this stage to argue on the basis of the *EDPS v SRB* judgment that pseudonymisation always lead

to anonymisation when the receiving end is a controller. The CJEU judgment is nuanced: while it foresees the possibility of anonymisation at the receiving end, it suggests that a reidentification risk assessment should be performed and may not always lead to the conclusion that anonymisation has been achieved. The CJEU judgment thus offers a better reasoning than the General Court judgment.

However, two weaknesses are worth mentioning: the focus upon anticipated recipients as mentioned above, and the use of the term impersonal, which may cause unnecessary confusion. The CJEU described IP addresses (at issue in [Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14](#)) and vehicles identification numbers (at issue in [Scania CV AB, Case C-319/22](#)) as impersonal data: although these data points do not relate to natural persons by content, they are likely to do so by purpose and can therefore be considered at least indirect, if not direct, identifiers, they relate

to a closed group of individuals.

**2. The *EDPS v SRB* judgment should be complemented by regulatory guidance:** The CJEU does not provide all the elements needed for a risk assessment, which is where regulatory guidance remains important. Framing the assessment in terms of a motivated intruder test, as suggested by the ICO in its anonymisation guidance, is useful for at least three reasons: it stresses that threat modelling is a key initial stage and that the release model (closed or open) matters; that all situationally-relevant attackers should be taken into account, including unanticipated recipients; and that both technical and organisational measures will be needed to achieve anonymisation.

Importantly, the CJEU’s framing is compatible with the EDPB’s framing in its pseudonymisation guidelines. At the core of the pseudonymisation guidelines lie the concept of a pseudonymisation domain, which is configurable by the controller. This allows the pseudonymisation process to be more or less robust. “The pseudonymisation domain does not have to be all-encompassing, but may be restricted to defined entities, most often to the set of all authorised recipients of the personal data that will process the data for a given purpose”, wrote the EDPB.

Further, assuming one does not read too much into the EDPB’s guidelines, it is possible to explain the following statement in the light of *EDPS v SRB*: “If pseudonymised data and additional information could be combined having regard to the means reasonably likely to be used by the controller or by another person, then the pseudonymised data [are] personal. Even if all additional information retained by the pseudonymising controller has been erased, the pseudonymised data become anonymous only if the conditions for anonymity are met”.

What this paragraph should mean is that as, a matter of principle, all situationally relevant attackers are in scope for an anonymisation claim, although in some cases, controllers may be deemed trusted and therefore excluded from the list of situationally relevant

—  
**“It would be risky and inappropriate at this stage to argue on the basis of the *EDPS v SRB* judgment that pseudonymisation always lead to anonymisation when the receiving end is a controller. The CJEU judgment is nuanced: while it foresees the possibility of anonymisation at the receiving end, it suggests that a reidentification risk assessment should be performed and may not always lead to the conclusion that anonymisation has been achieved.”**  
 —

*(Continued from page 9)*

attackers. Deletion of additional information is no guarantee that the risks of reidentification associated with pseudonymised data have been fully mitigated, as e.g., publicly accessible data could enable identification.

Anonymisation requires a risk assessment, and thereby the definition of a threat model and a set of control measures adapted to the threat model.

In its overview of its case law, the CJEU referred both to *Breyer* (see above) and IAB Europe (*IAB Europe v Gegevensbeschermingsautoriteit, Case C-604/22*). It is important to preserve as much as possible the contribution of IAB Europe, as IAB Europe sets the outer limits of identifiability in cases of profiling. This case suggests that unique references that may not relate by content to natural persons (but certainly by purpose) may be enough to characterise identifiability in certain cases. To use the words of the CJEU in *IAB Europe*: “In the second place, it is also common ground that, where the information contained in a TC String is associated with an identifier, such as, inter alia, the IP address of the device of such a user, that information may make it possible to create a profile of that user and actually identify the person specifically concerned by such information”.

Finally, it is interesting to see that the CJEU grounded its ‘whose hands’ approach to anonymisation in the OC judgment (*OC v European Commission, Case C-479/22 P*). In that judgment, the CJEU sanctioned an extremely weak decision on the part of the General Court, stating strongly that “for information to be treated as ‘personal data’, it is not required that all the information enabling the identification of the data subject must be in the hands of one person” and that “the fact that additional information is necessary to identify the data subject does not mean that the data at issue cannot be classified as personal data”.

One important error that the General Court had committed in OC was that it had not considered publicly accessible information to determine what the

means reasonably likely to be used by the public were. What the OC judgment shows is the importance of adopting a proper threat model when attempting to anonymise the data and such threat model may include attackers with prior knowledge.

### **3. The EDPS v SRB judgment may not solve all divergences just yet:**

One issue not explicitly resolved by the CJEU is whether singling out, e.g., the presence of unique person-level records in a table, necessarily precludes anonymisation. In *EDPS v SRB*, some comments had been generalised and could therefore be linked to a group of individuals, while others were unique. The inclusion of unique comments in the data shared with Deloitte was not treated by the CJEU as a relevant factor when assessing the potential effect of pseudonymisation.

This position is sensible and, despite contrary interpretations by some supervisory authorities (‘SAs’), for example the Italian SA in the ‘Thin Database’ case (a 2023 decision), it is consistent with the opinion of the EDPB’s predecessor on anonymisation techniques, which allowed for a thorough evaluation of risks where singling out, linkability, or inference could not all be satisfactorily mitigated. That said, it should be clear that singling out remains an important component of any re-identification risk assessment, if not the main in cases of profiling, and some form of generalisation and randomisation are likely to be required to achieve anonymisation. It remains to be seen how national SAs will respond to this issue.

## **Conclusion**

The *EDPS v SRB* judgment is not surprising. It lays the foundation for a long-awaited uniform approach to anonymisation, comparable to variants adopted in other jurisdictions, such as under the UK GDPR or the US Health Insurance Portability and Accountability Act and its expert determination test. It also aligns with the approach taken by the European Medicines Agency in its external guidance on the implementation of the European Medicines Agency Policy

0070 on the publication of clinical data for medicinal products for human use. Going forward, SAs should ensure that they provide useful guidance on accepted methodologies for assessing residual re-identification risks in context, and confirm that distinguishability is enough to characterise identifiability in cases of profiling.

---

**Sophie Stalla-Bourdillon**

Brussels Privacy Hub

Sophie.Stalla-Bourdillon@vub.be

---