Sophie Stalla-Bourdillon
Brussels Privacy Hub, VUB, Brussels

Response to Consultation 01/2025 Guidelines on Pseudonymisation

This response builds upon the following publications:

1. Stalla-Bourdillon, S. (Accepted/In press). Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU? *European Journal of Risk Regulation*. 29 p.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5118064

2. Stalla-Bourdillon, S. (2025). The EDPB 01/2025 Guidelines on Pseudonymisation: A Step in the Right Direction? *European Law Blog*.
https://www.europeanlawblog.eu/pub/tfef074h/release/1

3. Stalla-Bourdillon, S. (2025) The State of Pseudonymisation in the EU: Where do we stand today? Privacy and Data Protection 25(2).
The state of pseudonymisation in the EU: Where do we stand today? - Vrije Universiteit Brussel

Although this response welcomes the Guidelines, it highlights several internal inconsistencies that occasionally make the Guidelines difficult to understand. Aiming to contribute to the development of a more robust framework for assessing identifiability, this response also identifies key areas of convergence between the approaches of the EDPB and the CJEU and offers a reading of the Guidelines in the light of the recently delivered opinion of the Advocate General (AG) Spielmann in *EDPS v SRB*.[1]

1. Inconsistencies within the Guidelines

The first conceptual challenge emerging from the Guidelines comes from the confusion that is made between the 'identifiability' and the 'relating to' criteria. The EDPB's predecessor had broken down the Data Protection Directive's definition of personal data into a four-prong test in its 2007 Opinion on Personal Data:[2] 'any information', 'relating to', 'identified or identifiable', 'natural person.' Pseudonymisation as a data transformation technique that aims to pursue (at least in part) the data protection principle of confidentiality, has no implication for the appreciation of the 'relating to' criterion which tries to answer the question whether the data describes an individual or something else, like an event, or a machine, or say an animal. As such, pseudonymisation only impacts

[1] *EDPS v SRB* [2025] Advocate General Spielmann Case C-413/23 P, ECLI:EU:C:2025:59.
[2] Article 29 Data Protection Working Party, 'Opinion Nº 4/2007 on the Concept of Personal Data' (2007) WP136 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp134_en.pdf>.

the identifiability level associated with the individual record. It is therefore confusing to write that "to attribute data to a specific (identified) person means to establish that the data relate to that person." (para. 17)

A more precise formulation would be: '[a]ttributing data to a specific individual means determining that the individual is either identified or identifiable based on the data available within the pseudonymisation domain."

The technical literature on de-identification usually draws a distinction between direct and quasi (or indirect) identifiers to explain the difference between direct and indirect identifiability, which seems to be at the heart of Article 4(1) GDPR. Although the EDPB draws a distinction between direct and quasi-identifiers, the terminology could appear confusing. The EDPB defines direct identifiers as essentially distinguishing references. However, a pseudonym is by definition a unique reference and therefore distinguishing. This would mean that pseudonymised data is always directly identifying, which is not exactly what that EDPB is trying to say about pseudonymised data. At para. 8, the EDPB writes that "it is clear that direct identifiers need to be removed from data if those data are not to be attributed to individuals." To make sense of what the EDPB is saying, one would need to add that certain types of direct identifiers are not identifying, which is a confusing assertion.

A better formulation would therefore imply acknowledging that direct identifiers have two key characteristics: distinguishability (i.e., uniqueness) and availability (they are potentially available or accessible to or by an attacker). When appropriate data segmentation measures have been implemented, and considering the pseudonymisation domain only, pseudonyms should not be considered available.

For the sake of clarity, it may help to include two sets of definitions: one for direct identifiers and one for quasi or indirect identifiers.

One last point on international data transfers. As explained in a prior paper, the description of what pseudonymisation processes should look like in the context of international data transfers seems to suggest that no thorough evaluation of the risks is ever possible in this context.[3] If this is true, a more detailed explanation as to why this is the case would be useful.[4] It maybe that the EDPB assumes that third-party public authorities should be considered as having some form of prior knowledge, which makes a thorough evaluation of the risks particularly challenging, but this is not explained in these terms.

[3] Sophie Stalla-Bourdillon and Alfred Rossi, 'The Technical Fix for International Data Transfers - a Word of Caution' (2021) 21 Privacy and Data Protection 6.
[4] Sophie Stalla-Bourdillon, 'Cross-Border Data Transfer Tools v Privacy Enhancing Technologies: A False Debate' (Cerre 2024) <https://cerre.eu/wp-content/uploads/2024/09/CBDT_FullBook_FINAL.pdf>.

2. Compatibility with CJEU Case Law

Many have criticised the EDPB Guidelines stating that it relies upon a misconception of the legal test for identifiability.

While it is true that the EDPB does not perform an analysis of the CJEU case law, the EDPB's approach and that of the CJEU as it stands today do not seem to be misaligned. Truly, the CJEU is still in the process of refining the identifiability test under the GDPR, as an appeal judgment on this matter is still expected in the SRB case.[5]Looking at the CJEU case law on identifiability though,[6] there seems to be a way to make sense of both the CJEU case law and the EDPB approach to pseudonymisation and arguably anonymisation as well. This can be done by referring to the concepts of distinguishability and availability introduced earlier. Let's explain.[7]

In Opinion 01/2025, the EDPB is essentially saying (assuming it manages to streamline its definitions) that within the pseudonymisation domain, pseudonyms are distinguishing but not available. As a matter of principle, this does not exclude that if a thorough evaluation of the risks is conducted, transformed data within an anticipated recipient's controlled environment could never be considered anonymised. However, until such a demonstration is made—bearing in mind that the burden of proof lies with the party claiming the anonymised status—the data should be regarded as pseudonymised. What is more, feedback loops, i.e., whether it is anticipated that the pseudonymised data will enrich the original data at some point in time, are also relevant for the analysis. Each time a feedback loop is maintained between the original data and the pseudonymised data, there are good reasons to adopt a holistic approach for the legal assessment and not to artificially separate the pseudonymising entity's hands from the data recipient's hands.

Of note, in *SRB* there is no demonstration that a thorough analysis of risks has been performed and there is a feedback loop that is maintained between the original data and the transformed data.

In *Breyer*[8] and *Scania*,[9] the CJEU considers the status of two types of data points: dynamic IP addresses and Vehicle Identification Numbers (VINs). Importantly, IP addresses and VINs are not pseudonyms as the EDPB views them. What is more, in *Breyer*, dynamic IP addresses are considered to be both distinguishable (singling out

[5] *Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS)* [2023] General Court Case T-557/20.
[6] Assuming we do not consider the General Court's judgment in *SRB*.
[7] For a detailed overview of the CJEU case law through the lenses of these two concepts see Sophie Stalla-Bourdillon, 'Identifiability as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU?' (2025) Forthcoming European Journal of Risk Regulation.
[8] *Patrick Breyer v Bundesrepublik Deutschland* (2016) ECLI:EU:C:2016:779.
[9] *Gesamtverband Autoteile-Handel eV v Scania CV AB* [2023] CJEU C-319/22, ECLI:EU:C:2023:837.

takes place) and available (the data holder, i.e., an online service provider, has the legal means to access additional identifying information). In *Scania*, VINs are considered indirect personal data in the hands of vehicle manufacturers, which is essentially implying that they are distinguishing and potentially available to anticipated recipients, i.e., independent operators.

In *IAB Europe*,[10] the CJEU adds a very important nuance, which suggests that the concept of personal data is rightly functional.[11] When the anticipated processing implies or enables the profiling of data subjects, the only criterion that matters is distinguishability. What this implies is that a thorough evaluation of the risks is in this case irrelevant, which aligns with a high level of data protection.

And in Bindl, although the General Court's reasoning lacks nuances, the description of the last disputed data transfer seems to imply that the IP address at stake is both distinguishable and available.[12]

3. Reading the Guidelines in the light of the AG's opinion in EDPS v SRB

The AG's opinion in *EDPS v SRB*[13] tackles the legal effects of pseudonymisation in at least two different ways.

First, the AG confirms very clearly that the 'relating to' prong of the definition of personal data is distinct from the 'identifiability' prong and, implicitly, that pseudonymisation has not impact upon the 'relating to' prong. Indeed, while the AG has no problem finding that the data held by Deloitte is at least pseudonymised, he states that the comments do relate to natural persons. At para. 33 and 34, the AG writes that:

- "[i]n the absence of proof to the contrary, the comments at issue in the present case, since they emanated from the complainants and showed 'their logic and reasoning', thus reflecting the expression of their 'subjective opinion', necessarily 'related' to those complainants, irrespective of the purpose or effect of their comments."
- "In any event, even in the absence of such a presumption in the present case, I am of the opinion that the comments at issue 'relate' to the complainants by reason of their content, purpose and effect."

Such a view echoes the critique of the EDPB Guidelines developed in the first section.

Second, the AG opines that pseudonymised data may amount to anonymised data. At para. 51 and 52, the AG writes that:

---

[10] *IAB Europe v Gegevensbeschermingsautoriteit* [2024] CJEU C-604/22, ECLI:EU:C:2024:214.
[11] Stalla-Bourdillon (n 7).
[12] *Bindl v European Commission* [2025] General Court T-354/22, ECLI:EU:T:2025:4.
[13] *EDPS v SRB* (n 1).

- The wording of Recital 16 "leaves open the possibility that the data subjects may not be identifiable, otherwise the wording of recital 16 of that regulation would be pointless."
- Under Recital 16 there is no reason to rule out that pseudonymised data "may, under certain conditions, fall outside the scope of the concept of 'personal data'."

Of note, Recital 16 of Regulation 2018/1725 is essentially a copy of GDPR Recital 26.

If such a view is confirmed by the CJEU, this would mean that one should not read too much into the EDPB Guidelines. With this said, as explained by the AG himself, the CJEU does not need to go that far to solve the case.

The AG opinion is however problematic in three ways.

The identifiability test that is emerging from the AG opinion appears confusing. At para. 57, the AG states that "it is only where the risk of identification is non-existent or insignificant that data can legally escape classification as 'personal data'." Yet, it is not good practice to only look at the means available to the anticipated data recipient to make such an assessment, unless the AG implies that considering the means of the anticipated recipient also means considering whether the anticipated recipient has performed a robust security assessment to appropriately mitigate against attacks from unanticipated third parties, which would require defining a relevant threat model and selecting a set of effective controls. Adopting a robust identifiability test is critical in the light of the newly adopted data sharing mandates.

Moreover, the AG does not account for any feedback loop present in *EDPS v SRB*. Yet, there is a strong argument that when such a feedback loop exists, it no longer makes sense to separate the party responsible for the data transformation process from the party receiving the transformed data. A feedback loop occurs when the intended use of the transformed data suggests that it will ultimately be linked back to identifying data or used to assess the situation of natural persons. This appears to be the case in *EDPS v SRB*. Therefore, one could argue that Deloitte's processing is merely ancillary to that of the SRB and should not be artificially segmented.

Finally, the AG could be read as suggesting that when a party alleges that it holds anonymised data, the EDPS bears the burden of establishing "for what reason, legal or technical, the pseudonymisation process (…) was not sufficient and should have led to the conclusion that [the data recipient] was processing personal data." (para. 96). Such a stance is problematic, in particular in the light of the newly adopted data sharing mandates. A better approach should be that the party alleging that it holds anonymised data should perform that demonstration, which could then be accepted or rejected by the EDPS but once a systematic and documented approach has been submitted to the EDPS.

Going further, there is also little consideration of the effects of Article 12 (the equivalent of Article 11 GDPR), which provides that when the controller is able to demonstrate that it is not in a position to identify the data subject, most of the data subject rights do not apply except where the data subject provides additional information enabling his or her identification. Under Article 12 it is the for the data controller to demonstrate that it is not a position to identify the data subject.