Date: 11-03-2025

Reaction to Guidelines 01/2025 on Pseudonymisation

Clear guidelines on the topic of pseudonymisation are very much needed, as many questions remain, particularly regarding the relationship between pseudonymisation and anonymisation. As the opinion on anonymisation techniques[1] by the Article 29 Working Party now dates back a decade, and the opinions on anonymity expressed therein are at odds with more recent case law of the CJEU, clarity on this issue is essential, in particular for member states which adhere to the 'consent or anonymise' dichotomy regarding scientific research.

However, in their current form, these draft guidelines fail to address recent case law and even appear to tacitly endorse the WP29 opinion on anonymisation. The possibility of pseudonymised data being personal data in the hands of one party and anonymous data for another is not only ignored, but also seemingly dismissed.

As a result, the guidelines risk expanding the scope of personal data, contrary to the case law of the CJEU. Opinions and guidelines of the EDPB are soft law, which, although not legally binding, are supposed to increase legal certainty. It is therefore disappointing that in their current form these guidelines have achieved the opposite.

Case law of the CJEU

The guidelines define and breakdown 1) what effective pseudonymisation entails, 2) the objectives and advantages of pseudonymisation, and 3) the technical measures and safeguards for pseudonymisation. In addition, a number of examples of the application of pseudonymisation are given to illustrate its use and benefits.

In light of these contents, it is noteworthy that no mention is made of either Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14) or SRB v EDPS (Case T-557/20) of the Court of Justice of the European Union.

The Breyer case clarified the circumstances under which a dynamic IP address constitutes personal data. The determination hinged on whether the data could be linked to an identifiable individual by the "means likely reasonably to be used."

[1] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (10 April 2014).

Importantly, this did not equate to means explicitly prohibited by law or those requiring disproportionate effort in terms of time, cost, or manpower.[2]

In the case of SRB v EDPS, the Single Resolution Board (SRB) invited shareholders to submit comments regarding its activities. These comments were coded and subsequently shared with a third party, Deloitte. A few shareholders subsequently complained to the EDPS that SRB had failed to inform them that personal data relating to them would be transmitted to third parties, in breach of the terms of the privacy statement. On this, the EDPS agreed. Subsequently, the SRB appealed to the General Court. The Court determined that the EDPS had failed to demonstrate that the coded data held by Deloitte was in fact personal data. According to its decision, it is always necessary to assess whether a data recipient is reasonably able to re-identify the data subjects. The EDPS should have investigated whether Deloitte had the legal means which could in practice enable it to access the additional information necessary to re-identify the data subjects.[3]

The approach to anonymity expressed in these two cases is often referred to as the relative approach to anonymity, meaning that who has access under which circumstances matters in determining whether data can be considered anonymous. In this view, data can be anonymous for one party, and personal data for another party.[4]

This approach differs from the approach to anonymity expressed in Opinion 05/2014, often referred to as the absolute approach, which considers the nature of the data to be decisive irrespective of who has access to the data under which circumstances.

However, the draft guidelines seem to sidestep the conflict between these approaches. The guidelines do address the issue of determining the anonymity of data, but unfortunately fail to offer any clarity:

"*Pseudonymised data, which could be attributed to a natural person by the use of additional information, is to be considered information on an identifiable natural person, and is therefore personal. This statement also holds true if pseudonymised data and additional information are not in the hands of the same person. 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 is personal. Even if all additional information retained by the*

[2] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, [2016], ECLI: EU: C: 2016: 779, par. 46.
[3] Case T-557/20, Single Resolution Board v European Data Protection Supervisor, [2023], ECLI:EU:T:2023:219, Par. 105.
[4] See also Case C-319/22, Gesamtverband Autoteile-Handel eV v Scania CV AB, [2023], ECLI:EU:C:2023:837, par. 49.

pseudonymising controller has been erased, the pseudonymised data becomes anonymous only if the conditions for anonymity are met."[5]

In the above paragraph, only the nature of the data is being taken into account, and consequently, the court's judgement in SRB v EDPS that the question of whether pseudonymised data in the hands of a third party qualifies as personal data should be considered from the perspective of that third party[6] is ignored. Furthermore, on the conditions for anonymity mentioned in the last sentence of the above paragraph we would expect these guidelines to provide more information.

Pseudonymisation domain

The draft guidelines also introduce the concept of the pseudonymisation domain, the environment in which the controller or processor wishes to preclude attribution of data to specific data subjects:

"*Controllers may define the context in which pseudonymisation is to preclude attribution of data to specific data subjects, generally on the basis of a risk analysis. They subject the additional information to technical and organisational measures to ensure that the pseudonymised data cannot be attributed to data subjects by persons operating within that context. This means in particular that additional information that would enable attribution is kept separate from it. These guidelines call this context (with the people operating in it and its attending physical and organisational aspects, including the IT assets available) the pseudonymisation domain*."[7]

In our understanding, the pseudonymisation domain consists of the objective of why data are pseudonymized and by what measures (cryptography or using lookup-tables with other identifiers), and is therefore key in determining the level of security appropriate to the risk of attributing pseudonymised data to specific individuals. But whether it is possible for data to be considered anonymous within the context of the pseudonymisation domain for third parties remains unclear.

Application of pseudonymisation

The draft guidelines offer 10 examples of the application of pseudonymisation, of which a few contain the scenario in which a controller discloses pseudonymised data to a third-party recipient. Examples 3, 4, 5, and 6 are related to healthcare.

Notably, none of these examples clarify if and how measures could be implemented that would allow a third party to demonstrate that it is not reasonably likely to identify a

[5] Draft guidelines 01/2025 on Pseudonymisation, par. 22.
[6] Par. 97.
[7] Draft guidelines 01/2025 on Pseudonymisation, par. 35.

natural person in the received dataset and that the data could therefore be considered anonymous for the receiving party.

Example 5 offers the example of a data centre which, as part of a research project receives health data from participating university hospitals and collects data about occupational exposure to health hazards from a Labour agency. The example explains how the data centre provides the results of queries on the data to research groups, while preventing attribution of the data by those same research groups. The data access board seeks contractual guarantees from the receiving research group that all members are prevented by technical and organisational safeguards from access to any additional information that would allow attribution of the pseudonymised data to data subjects. However, it remains unclear if there are circumstances in which the data the research group receives could be considered anonymous for that research group.

The pseudonymisation domain in relation to the EHDS

Given the introduction of the pseudonymisation domain, it is also noteworthy that no mention in the draft guidelines is made of the secure processing environment (SPE) in which electronic health data will be processed under the European Health Data Space (EHDS). An SPE, as defined in the Data Governance Act, is a physical or virtual environment and organisational means to ensure compliance with Union law, in particular with regard to data subjects' rights, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms.[8]

Under the EHDS, all secondary use access to electronic health data should be done through an SPE, which will reduce the privacy risks related to such processing activities and prevent the electronic health data from being transmitted directly to the health data users. Only aggregated data can be downloaded by the health data users from an SPE.

Due to the EHDS, we can expect a considerable degree of scientific health research to take place in such SPE's in the near future. The EHDS may make the discussion on anonymity largely superfluous. However, systems of data sharing parallel to the EHDS will still be allowed, and many Dutch research institutions already employ SPE's.[9] It would therefore be helpful for the EDPB to provide guidance on the conditions under which data within an SPE can be considered anonymous for the health data user.

[8] Art. 2, point 20, Regulation (EU) 2022/868.
[9] See for instance the remote access facility of Statistics Netherlands: https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen

Our conclusion

To conclude, our concerns regarding the draft guidelines are as follows:

- In our opinion, and from a data protection perspective, pseudonymisation is closely intertwined with anonymisation. Therefore, we would expect the EDPB to provide guidance on both concepts in one guideline;
- The court's judgement in the Breyer case and SRB v EDPS that whether pseudonymised data in the hands of a third party qualifies as personal data should be considered from the perspective of that third party is ignored;
- As a result, this creates a risk that these guidelines differ from the conclusions by the court, and will lead to legal uncertainty with regard to the application of pseudonymisation in practice;
- The possibility of data being considered anonymous within the context of the pseudonymisation domain for third parties remains unclear;
- The examples mentioned in the annex do not clarify if and how measures could be implemented that would allow a third party to demonstrate that it is not reasonably likely to identify or re-identify a natural person in the received dataset and that the data could therefore be considered anonymous for the receiving party;
- Whether pseudonymised data processed within a secure processing environment can be considered anonymous for a health data user is not addressed.

The case of SRB v EDPS is still ongoing; the EDPS has appealed[10] against the judgement for having, in their view, incorrectly required the EDPS to assess whether the information at stake in the case was personal data taking the perspective of the recipient and by omitting to give consideration to the notion of pseudonymisation.

The opinion of Advocate General Spielmann[11] illustrates the existence of the two different approaches to the scope of data protection rules, and explicitly poses the question whether pseudonymised data should be included within that scope on the sole ground that the data subjects remain identifiable, irrespective of the accessibility of the additional identification data, or if it should be considered that data are personal data only for those persons who can reasonably identify the data subjects.[12] On this he clearly states that "*...pseudonymisation leaves open the possibility that the data subjects may not be identifiable*" and that "*if it is impossible to identify those data*

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2023.296.01.0024.02.ENG&toc=OJ%3AC%3A2023%3A296%3ATOC

[11] Case C-413/23 P, European Data Protection Supervisor v Single Resolution Board, [2025], ECLI:EU:C:2025:59, Opinion of Advocate General Spielmann, delivered on 6 February 2025.

[12] Par. 43.

subjects, they are therefore legally considered to be sufficiently protected by the pseudonymisation process, notwithstanding the fact that the additional identification data have not been completely erased."[13]

If the opinion of the AG is a harbinger of the conclusion to this case, the appeal of the EDPS will likely not succeed.

According to the EDPB work programme of 2024-2025, guidelines on anonymisation are still on the agenda, and these future guidelines may clear up some of the confusion addressed in this letter. However, a thorough examination of pseudonymisation necessitates addressing anonymisation as well—otherwise, a significant gap remains, as these draft guidelines unfortunately illustrate. Furthermore, given that we still await the final judgement on this case, the timing of these draft guidelines is remarkable. It would enhance legal certainty if the guidelines were not issued until after the judgement is rendered.

Kind regards,

On behalf of

COREON

Health-RI

Nederlandse Vereniging voor Pathologie (NVVP)

Federatie Medische Specialisten (FMS)

Should there be any questions following this, please contact Daniel Groos, Partnership Manager at Lygature daniel.groos@lygature.org.

[13] Par. 51. The latter part of the sentence, which states: "*...notwithstanding the fact that the additional identification data have not been completely erased"* runs counter to the view expressed in the draft guidelines in par. 22: "*even if all additional information retained by the pseudonymising controller has been erased, the pseudonymised data becomes anonymous only if the conditions for anonymity are met*."