14 March 2025

EBF_046722

EBF response to the European Data Protection Board's consultation on the draft Guidelines 1/2025 on Pseudonymisation

Key points:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's (EDPB) consultation on the draft Guidelines on Pseudonymisation, hereinafter – the Guidelines.
- We welcome that the Guidelines clearly recognise the role of pseudonymisation in mitigating risks and limiting the possible consequences of the further processing of personal data for data subjects.
- We also welcome the intention of the EDPB to provide legal clarifications on the definition and applicability of pseudonymisation and pseudonymised data. However, **the EDPB must ensure that the Guidelines align with** current developments in the jurisprudence, particularly as regards the distinction between pseudonymised and anonymised data and the possibility for re-identification of data subjects. In light of **the upcoming judgment of the CJEU on pseudonymisation**, we therefore caution against adopting an absolute position.
- We would welcome if the Guidelines could provide examples as to the practical application of the concept of "pseudonymisation domain", as well as consider adding in the Annex examples of the use and benefits of pseudonymisation for the sector as proposed by our experts.

Section 2: Definitions and legal analysis

2.1 Legal definition of pseudonymisation

In the Guidelines, the distinction between pseudonymised and anonymised data is not always clear, which may create confusion. We would welcome if the EDPB could strengthens the distinction between the two terms with concrete examples illustrating the criteria for identifying genuinely anonymized data and their practical usage. We also recommend that these Guidelines do not contradict the forthcoming guidance on anonymisation (announced in the EDPB Work Programme 2024-2025).

Under **Paragraph 22**, the Guidelines suggest that pseudonymised data is always to be considered as personal data, even in the event where third-parties do not possess the keys for re-identification. We note, however, that **discussions around the risk of re-identification and the nature of pseudonymised data when in the hands of a data**

recipient who doesn't have the additional information are fast evolving.[1] As some uncertainty remains on the nature of pseudonymised data, **we recommend that the EDPB temporarily refrains from adopting a standpoint in this regard but awaits for the upcoming judgment of the CJEU**.

We would also appreciate if the EDPB could provide more guidance on the concept of "*reasonable likelihood*" of re-identification, and clarify the application of the "reasonable likelihood" test in the event that A) the sender and recipient of the data are autonomous legal entities not belonging to the same "Corporate Group" and B), alternatively, when both sender and recipient belong to the same "Group". We suggest clarifying that a Corporate Group has the choice of having recourse to different technical and organisational measures to assess what the reasonable likelihood of re-identification may be. We propose including the following examples for our sector. Specifically, it would be important to clarify how "reasonable" it is for two companies of the same "Group" to claim that the re-identification keys are in no way accessible to the recipient of the data.

2.3 Pseudonymisation domain and available means for attribution

While we welcome the intention of the EDPB to clarify the concept of "pseudonymization domain", which is well-developed and frequently referenced throughout the document, we would like to highlight that understanding the domain requires advanced technical skills. We would therefore appreciate it if the EDPB could **include practical examples in Section 2.3 to facilitate the application of the concept**, particularly for smaller organizations or those with limited resources.

2.4 Meeting data-protection requirements using pseudonymisation

2.4.1.3 Lawfulness, fairness and accuracy principles

We would welcome further clarification on **how pseudonymisation can be used** in relation to the processing of personal data based on **legitimate interest**, either under Chapter 2.4.1.3 or as an example in the Annex, in addition to the Example 7 already provided.

2.4.3 Pseudonymisation as a supplementary measure for third country data transfer

The use of pseudonymization as a "supplementary measure" for transfers to third countries seems effective only in theory. As mentioned in **Section 2.4.3**, with particular reference to **paragraph 65**, it is unclear how the concrete applicability can be measured for which "*any design of a pseudonymisation procedure needs to start from an assessment of which information the public authorities of the recipient country can be expected to possess or to be able to obtain with reasonable means, even if those means may infringe the legal norms in the third country*". **What measures would ensure that additional information remains inaccessible to foreign authorities or other third parties?** Also, depending on the upcoming decision of the CJEU, it may be argued that, in certain circumstances, if for the recipient in a third country the risk of re-identification is "non-existent or insignificant", it could be that for that recipient those data fall outside the scope of the GDPR, which would facilitate such transfers.

[1] On April 26, 2023, the General Court of the European Union issued its judgment in Case T-557/20, SRB v EDPS. The case, however, is currently pending before the CJEU (C-413/23 P), and the Advocate General issued their opinion on February 6, 2025.

2.6 Implications for the rights of the data subject

Paragraph 77 appears to imply that Article 11 GDPR only applies in those instances where the controller is not able to (re)identify the data subject. For example, because it does not have access to the additional information that allows identification. It is unclear, however, whether these considerations also apply to cases where a data controller has access to "additional information". In this regard, if a data subject requests access to their data, as per Article 15 GDPR, how is the data controller expected to process the request? For the purposes of complying with Article 15, should the controller request the information from both the organizational unit that constitutes the pseudonymization domain and the organizational unit that has the additional information or would it be more appropriate not to interfere with the pseudonymization domain, but rather have the additional information provided directly by the data subject (as per art. 11, para. 2 GDPR)? All in all, these steps regarding the re-identification may require additional effort and time.

It should also be noted that the example provided in **Paragraph 78** does not apply to banks. For example, to comply with the anti-money laundering (AML) legislation, our industry cannot accept clients that only provide a pseudonym and not the required personal information. We therefore recommend including a footnote specifying that the example provided in Paragraph78 does not apply to obliged entities acting in compliance with their obligations under financial sector-specific legislation.

The recommendation under **Paragraph 79** should not apply to the sector either. This example should not imply that individuals have the right to obtain the pseudonyms used by the bank to protect the data, since this would constitute a security breach.

3. Technical Measures and Safeguards for Pseudonymisation

3.1.2 Types of pseudonymising transformations

Paragraph 93 briefly addresses the issue of cryptanalytic attacks – and the susceptibility to such attacks. However, the Guidelines do not adequately explore the level of protection pseudonymization provides against sophisticated re-identification attempts, especially when attackers have access to additional data sources. A point in case is **Paragraph 93**, which states that "*[…] controllers need to weigh the disadvantage of securely storing this possibly large set of personal data against the reduced or avoided* ***susceptibility to cryptanalytic attacks*** *in comparison to the first class of procedures, which is particularly important wherever long-term guarantees for irreversibility of the pseudonymising transformation are needed*". What guarantees exist regarding the effectiveness of pseudonymization against such threat scenarios?

Annex – Examples of the Application of Pseudonymisation

We welcome the intention of the EDPB to clarify the use and benefits of pseudonymisation by way of real-world examples. However, the scenarios provided focus on limited areas - mainly healthcare and research. Indeed, other sectors relevant to business operations, including marketing, retail, and finance, would benefit from being included in the list of examples. We therefore **recommend that the EDPB diversifies the examples provided in the Annex by including more sectors and operational cases**, as this would ensure greater completeness and practical utility for our sector.

We note that the banking sector has acquired experience in the development and adoption of pseudonymisation techniques. We include below a number of

examples provided by experts in the field. Please note that, depending on the characteristics and the number of parties that could access the pseudonymised data, some of these techniques would be more suitable than the others.

- **Example 1**: Pseudonymize the data with hashing+secret-key (like HMAC-SHA2 or HMAC+SHA3). Without the secret key the pseudonymized data cannot be decrypted. The original data is needed to link it back to the individual. The secret key can be shared but every sharing of such key gives risks of leaking the key. Therefore, this technique is most suited for and should be limited to a small group of participants (e.g. max 5-7 mature parties/organisations).
- **Example 2**: Multi-Party computation techniques. This allows for multiple parties to share data for computing tasks without revealing each other's data. This can be used for a bigger group of participants.
- **Example 3**: Pseudonymize the data with hashing techniques (like SHA2 and SHA3). In the experience of our experts, this should not be used for "short length data" like credit card numbers. The reason is that "short lengths data" allow recalculation to the original data.

We also note that, in our sector, pseudonymisation can be implemented in certain scenarios to protect customer data when no identifiable information is need. For example, instead of processing customers' identification data, such as for analysis activities for statistical purposes, direct customer identifiers can be replaced with unique codes that prevent the identification of data subjects. **This allows data to be analyzed without directly exposing personal information, reducing the risk of unauthorised access and limiting access to identifiable information only when strictly necessary**.

Our experts on the field recommend developing and applying the above techniques in such a way that they are protected against Quantum Computer attacks to mitigate the 'Store now, decrypt later' risks. The recommendation would be to use the latest cryptographic algorithms and technics for this.

There are other techniques to pseudonymize data, however, not all of them are fit to be used to share bigger amounts of data. Some of these may be at the moment very costly or their implementation may imply significant organisational impact.

Finally, we suggest supplementing the existing examples on how pseudonymisation can be used in connection with the testing of IT systems, general data minimisation purposes, and further processing with compatible purposes.

Additional Elements for Consideration

- **Consistency with other GDPR tools**: while pseudonymisation is described throughout the Guidelines as a security measure, its relationship to other GDPR compliance tools, such as Data Protection Impact Assessments (DPIAs) or Standard Contractual Clauses (SCCs), is unclear. We would appreciate it if the EDPB were to clarify how pseudonymisation integrates with DPIAs and Transfer Impact Assessments (TIAs), for example, by providing guidance on how to evaluate it as a mitigation measure or by explaining its role in contracts with data processors.
- **Obligations of Data Processors and Third Parties**: The Guidelines attribute most responsibilities for the correct use of pseudonymisation to the data controller, while the roles of processors and third parties appear to be insufficiently detailed. We therefore recommend that the EDPB provides a more detailed description of

the processor's duties regarding pseudonymisation, including specific obligations such as assisting with data subject requests and ensuring data security, along with contractual references for third parties.

- **Aggregated data as a form of pseudonymisation**: We would also welcome further clarification concerning the concept of "aggregated data". While it is mentioned in the Annex (see p. 36 - "*Data from a given practice is analysed to provide aggregated data on the quality of care provided by this practice"*), there is no clear reference to this practice in the main body of the Guidelines, which raises questions as to whether this can be seen as a form of pseudonymisation.

ENDS

For more information:
Rachele Ceraulo
Project Coordinator – Data & Innovation
r.ceraulo@ebf.eu

About the EBF