EDPB Consultation on draft Guidelines 1/2025 on Pseudonymisation

INTRODUCTION

1. Pseudonymisation in data-driven marketing

FEDMA is pleased to provide its input to the European Data Protection Board's (EDPB) draft Guidelines 01/2025 on pseudonymisation. Pseudonymisation is a vital tool for data-driven marketing, enabling businesses to harness the power of data while safeguarding privacy and maintaining compliance with GDPR. By replacing identifiable information with pseudonyms, marketers can analyse customer behaviour, segment audiences, and deliver personalized experiences across multiple channels without directly identifying individuals. This approach reduces re-identification risks, ensures compliance with data minimisation and purpose limitation principles, and fosters consumer trust by protecting personal data. Additionally, pseudonymisation facilitates lawful data sharing with partners and advertising networks, enabling collaborative innovation while preserving data security. As data-driven marketing continues to evolve, pseudonymisation serves as a cornerstone for balancing effective marketing strategies with robust privacy protections. However, as these techniques are complex – it is therefore key to promote investment in these techniques so that they become accessible to more market players, including SMEs and start-ups that are key innovation drivers in data and AI.

Pseudonymisation techniques, while highly effective, are inherently complex and require significant technical expertise and resources to implement correctly. To ensure broader adoption and scalability, it is crucial to promote legal certainty, establish widely recognized technical standards, and encourage investment in these techniques. Clear regulatory guidance and alignment with international standards can provide businesses with the confidence to adopt pseudonymisation without fear of non-compliance. Additionally, fostering innovation in scalable and user-friendly pseudonymisation solutions will enable more market players, including SMEs and start-ups, to integrate these practices into their operations. Given their pivotal role as innovation drivers in the fields of data and AI, supporting smaller entities in adopting pseudonymisation can accelerate the development of privacy-preserving technologies while democratizing access to advanced data analytics.

2. The need for a balanced and future-proof approach to pseudonymisation

The pending *EDPS v. SRB* case before the Court of Justice of the European Union (CJEU) has the potential to significantly impact the interpretation of pseudonymisation under the GDPR. In his opinion, the Advocate General acknowledged that pseudonymised data in the hands of a data recipient could, in certain circumstances, be considered anonymised data. This position raises important questions about the distinction between pseudonymisation and anonymisation, which the EDPB's draft guidelines currently do not fully address. Given the potential implications of the upcoming CJEU ruling, we strongly recommend that the EDPB (i) refrain from publishing

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

the final version of the guidelines until the Court has issued its decision, or (ii) relaunch a public consultation if the ruling adopts a different approach than the one outlined in the guidelines, ensuring that the final version makes a clear distinction between pseudonymisation and anonymisation. An overly restrictive approach to pseudonymisation could have unintended consequences, discouraging the adoption of this crucial privacy-enhancing technique and limiting its potential benefits. This is particularly relevant in the context of Artificial Intelligence, where pseudonymisation plays a key role in enabling data-driven innovation while safeguarding individuals' privacy. By ensuring a balanced and future-proof approach, the EDPB can foster both regulatory clarity and the broader adoption of pseudonymisation as a tool for responsible data processing.

In this context, FEDMA provides the following recommendations:

1. Aligning the definition of personal data and reasonable means with relevant case law
2. Setting a workable definition of "additional information"
3. Explaining the notions of re-identification risk and residual risk
4. Providing guidance on testing robustness of pseudonymisation techniques
5. Clarifying data subjects' identity verification methods following pseudonymisation
6. Further exploring reliance on legitimate interest and pseudonymisation for data-driven marketing
7. Expanding the section on use cases of the guidelines to more sectors and processing
8. Avoiding an overinterpretation of Article 6(4) in contextual compatibility tests
9. Highlighting the role of pseudonymisation as a mitigating factor in enforcement
10. Ensuring alignment with international standards

RECOMMENDATIONS

1. Aligning the definition of personal data and reasonable means with relevant case law

The interplay between these guidelines and relevant case law is unclear, especially in relation to the relevant case law[1], pointing out that "personal data" is a relative concept. In its ruling, the CJEU adopted a risk-based approach in line with the GDPR, recognising that one must look at the means of identification "*reasonably likely to be used by the controller and any other person*" to determine whether certain information constitutes personal data. In contrast, paragraph 22, line 4 of the guidelines seems to suggest that pseudonymised data is always to be considered personal data even where a data recipient is not in possession of additional information for identification, regardless of his reasonable means of identification. This statement seems also to counter Recital 26 GDPR which confirms that where all objective factors do not indicate that a person is identifiable, the information should be considered anonymous data. Closer to this interpretation, paragraph 22, line 4-6 seems to re-introduce a more relative approach, considering the means reasonably likely to be used to combine pseudonymised data and additional information as per Recital 26 GDPR. We therefore recommend the EDPB to clear any confusion, also in light of the pending case EDPS v SRB, with the following amendment:

[1] Breyer v Germany [2016] C-582/14, para 42-49; Scania v European Commission [2023] C-319/22, para 45-49; IAB Europe [2016] para 49-51.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Draft Guidelines	Amendment
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.	*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 **may** also hold~~s~~ true if pseudonymised data and additional information are not in the hands of the same person.*

Another area of uncertainty stems from the nature of the reasonable means of identification by a third party that a data controller should take into consideration. On this point, the Breyer case clarified that 'reasonable' means *a practical possibility within the framework of the law* to access identifying data. Conversely, paragraph 42 of the guidelines refers to "both actions in good faith, and those executed with criminal intent"[2]. While we understand that the EDPB's additional consideration of "unlawful means" applies on a case-by-case basis according to *contextual elements and the circumstances at hands*, we recommend the EDPB:

- Clarify that while the sole consideration of legal means would ensure compliance with the legal framework, the additional consideration of "unlawful means" should be considered a best practice in certain circumstances, and
- Providing examples where a controller should take into account unlawful means of identification reasonably likely to be used by unauthorised third parties.
- Consider taking into account the notion of "good faith of the controller in complying with market standards".

2. Setting a workable definition of "additional information"

Article 4(5) GDPR defines pseudonymisation as processing that prevents attribution to a specific individual without the use of "additional information," which must be kept separately and protected by technical and organizational measures. This definition suggests that "additional information" refers to data already in the possession of the controller. However, paragraph 21 of the guidelines expands this notion by stating that controllers should also consider publicly accessible resources, such as social media posts or online forums, when assessing the effectiveness of pseudonymisation. This broader interpretation raises important questions about the extent of a controller's responsibility in evaluating re-identification risks. While factoring in publicly available data may enhance risk assessments, it also places an additional and potentially disproportionate burden on controllers, requiring them to anticipate and monitor external data sources beyond their direct control. Greater clarity is needed to ensure a balanced

[2] See also par. 37, 38, 60 which refer to unauthorised/not legitimate recipients

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

approach that maintains the integrity of pseudonymisation while setting reasonable expectations for compliance.

3. Explaining the notions of re-identification risk and residual risk

The guidelines could benefit from a more in-depth exploration of the notions of re-identification risk and residual risk, which are critical to assessing the effectiveness of pseudonymisation. Paragraph 35, for instance, merely stresses the need for a "risk analysis", but it does not go further in providing guidance on how to carry it out. Overall, the document emphasizes the need to secure additional information and evaluate potential attribution methods without providing a clear framework for assessing the likelihood and impact of re-identification in specific contexts. Furthermore, residual risk—representing the remaining risk after implementing pseudonymisation and other safeguards—is not thoroughly addressed. This leaves controllers with limited guidance on how to measure, mitigate, and document residual risks to demonstrate compliance with the GDPR's core accountability principle. We therefore recommend the EDPB to **add methodological clarity, possibly with concrete examples, on how to carry out such risk analyses**.

4. Providing guidance on testing robustness of pseudonymisation techniques

The guidelines do not address how controllers can test the robustness of their pseudonymisation techniques and validate their effectiveness for various use cases. Paragraph 47, for example, states that for pseudonymisation to be effective, individuals handling the pseudonymised data must, among other things, "not [be] able to single out the data subjects in other contexts on the basis of what they learned from handling the pseudonymised data." However, the guidelines do not define what constitutes "other contexts," leaving controllers without clear parameters for implementation. The EDPB should clarify this concept and provide **practical examples to ensure companies understand how to achieve effective pseudonymisation in practice**. Additionally, questions remain about whether such evaluations should be conducted through voluntary frameworks like codes of conduct, certifications, or regulatory sandboxes. **Providing clarity on standardized approaches for testing** would give controllers greater confidence in their compliance efforts and help ensure that pseudonymisation measures meet the intended levels of protection. It would also provide more upfront legal certainty and avoid that controllers only find that their pseudonymisation techniques meet or do not meet the expectations of the data protection authority at the enforcement stage.

5. Clarifying data subjects' identity verification methods following pseudonymisation

We urge the EDPB to provide **concrete examples illustrating how controllers can verify that the individual claiming data subject rights is indeed the person to whom the pseudonymised data relates**. This is a critical issue, as controllers must balance facilitating data subject rights with preventing unauthorized access to personal data. Some data protection authorities have shown reluctance to rely on national IDs to verify the data subjects' identity. In this context, the guidelines could explore practical solutions such as requiring the submission of pseudonyms or tokens generated during the pseudonymisation process, combined with additional proof of identity or contextual information. Other examples could include leveraging secure authentication mechanisms or cryptographic techniques to verify the individual's identity without compromising the security of pseudonymisation. Clear, actionable guidance in this area

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

would strengthen controllers' ability to uphold GDPR obligations while safeguarding against unauthorized disclosures.

Further guidance on this point is even more necessary in light of what seems to be a contradiction with the GDPR in paragraph 77. Article 11(1) GDPR establishes that if a controller can demonstrate that it is not in a position to identify a data subject, it is not required to maintain, acquire, or process additional information solely for the purpose of enabling the data subject to exercise their rights. This provision acknowledges that controllers applying effective pseudonymisation or other anonymization techniques should not be obligated to reintroduce identifiers into their systems. However, **paragraph 77 of the guidelines appears to take a different stance than the GDPR by implying that only when a controller cannot acquire the additional information to identify the data subject should it be exempt from such an obligation**. This interpretation risks contradicting Article 11(1) GDPR, as it could impose an expectation on controllers using pseudonymisation to actively seek identifying information rather than allowing them to rely on the principle that they are not required to do so. The EDPB should clarify this point to ensure that controllers using pseudonymisation are not placed under undue obligations that conflict with GDPR's original intent, thereby preserving legal certainty and promoting the adoption of privacy-enhancing measures.

Finally, Article 11(2) GDPR sets out the conditions preventing a data controller from complying with the GDPR to enable data subjects to exercise their rights under Articles 15 to 20 GDPR. As Article 11(2) GDPR does not foresee that the right to object may not apply, further clarification on identity verification in the context of pseudonymised data are extremely important.

6. Further exploring reliance on legitimate interest and pseudonymisation for data-driven marketing

We welcome the EDPB's view on how pseudonymisation can support both the legitimate interest balancing test under Article 6(1)(f) GDPR and the assessment of purpose compatibility under Article 6(4) GDPR. The acknowledgment that pseudonymisation can tilt the balancing test in favor of the controller and serve as a safeguard for further processing reinforces its role as both a security measure and a compliance tool. Example 8 specifically addresses a relevant use case on the use of pseudonymisation justifying further processing for data-driven marketing purposes. In this context, we encourage the EDPB to provide a more relevant example to illustrate the compatibility test under Article 6(4). Since health data requires explicit consent for being processing in the marketing context, the example is not suitable for illustrating a case for changing the processing purposes. In addition, it is common practice for business have legal basis to perform analysis of purchase history, hence most privacy policies contain the necessary transparency information to enable this. Using this example to illustrate the change of processing purposes can therefore be confusing. In this context, it would be useful to have additional **concrete and realistic examples where pseudonymisation makes it possible to strike a balance between the legitimate interests of the controller and the rights of data subjects**.

7. Expanding the section on use cases of the guidelines to more sectors and processing

It is encouraging to see the guidelines include multiple use cases demonstrating how pseudonymisation can be successfully applied to health data, a special category of personal

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

data that requires heightened protection under the GDPR. These examples showcase pseudonymisation's effectiveness in significantly reducing risks for data subjects, even in scenarios involving highly sensitive information. This seems to strongly indicate the potential of pseudonymisation to provide robust safeguards for use cases involving less sensitive data, where the risks are inherently lower. We nevertheless encourage the EDPB to provide **additional use cases in other sectors (health, finance, marketing, etc.) and types of personal data (health data, financial data, behavioural data, etc.)**, especially:

- Data sharing with marketing partners or advertising networks.
- Pseudonymised data for the development of AI and model training.

8. Avoiding an overinterpretation of Article 6(4) in contextual compatibility tests

While the guidelines highlight how pseudonymisation can contribute to the compatibility of further processing under Article 6(4), they also appear to presuppose that certain processing purposes, such as personalized advertising, inherently fail the compatibility test even when pseudonymisation is applied (Paragraph 48). This interpretation risks being overly rigid, as Article 6(4) explicitly requires a case-by-case assessment of compatibility, taking into account the specific context, safeguards, and measures in place. By making blanket assumptions about incompatibility, the guidelines may discourage innovative and compliant uses of pseudonymisation in contexts where further processing could align with GDPR principles if risks are appropriately mitigated. A more nuanced approach reflecting the contextual nature of Article 6(4) would provide greater flexibility and clarity for data controllers.

9. Highlighting the role of pseudonymisation as a mitigating factor in enforcement

While the guidelines thoroughly explore pseudonymisation as a technical and organizational measure to reduce risks for data subjects, they do not address its potential role in enforcement cases. Specifically, the guidelines miss an opportunity to clarify how the investment in pseudonymisation could be considered a mitigating factor by data protection authorities when evaluating a controller's compliance or imposing sanctions. **Recognizing pseudonymisation as a key risk-reduction measure in enforcement contexts could incentivize its adoption**, fostering stronger alignment between effective privacy safeguards and regulatory expectations. It is important to stress that the lack of consideration of investment in pseudonymisation as a mitigating factor could unfortunately have the effect of lowering the level of data protection on the ground if organisations are treated in the same manner, regardless of whether they process data in clear or in a pseudonymised manner.

10. Ensuring alignment with international standards

FEDMA points out a lack of **reference to existing international standards**, such as ISO/IEC 20889:2018 on pseudonymisation techniques and ISO/IEC 27559:2022 on privacy-enhancing data de-identification frameworks. These standards offer globally recognized benchmarks for implementing pseudonymisation effectively. By incorporating or aligning with such standards, the EDPB could promote consistency in data protection practices across jurisdictions and enhance interoperability for controllers operating in global markets. Ensuring alignment with international standards would strengthen the credibility and practical applicability of the guidelines.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org