EDPB Guidelines 01/2025 on Pseudonymisation

Telefónica Comments

March 2025

Telefónica welcomes the opportunity to respond to the European Data Protection Board's Guidelines 01/2025 on Pseudonymisation and the intention to provide clarification on the use and benefits of pseudonymisation. Pseudonymization of personal data stands as a fundamental tool in the field of data protection. As the EDPB demonstrates in its Guidelines, "*pseudonymisation is a safeguard that can be applied by controllers to meet the requirements of data protection law and, in particular, to demonstrate compliance with the data protection principles in accordance with Art 5(2) GDPR*." However, in addition to contributing to compliance, this technique also offers multiple advantages that can drive innovation in companies.

We do believe pseudonymisation plays a key role in artificial intelligence (AI) innovation and the optimization of emerging technologies, while respecting the protection of personal data. By transforming personal data into pseudonyms, the risks of identifying individuals directly are minimized, allowing organizations to use large volumes of data to train and improve AI models, without compromising the privacy of individuals. This approach not only facilitates compliance with regulations such as GDPR, but also promotes technological innovation by enabling the development of advanced solutions in areas such as telecommunications, medicine, education and other emerging technologies, without exposing more information than necessary. In this regard, we propose that the EDPB adopt a favorable position for the industry to work with pseudonymised data, thus facilitating technological innovation while ensuring lawful and ethical processing of the data.

In this document, Telefónica expands on some aspects of the draft EDPB Guidelines that need to be clarified in order to achieve a balanced outcome that provides real guidance for Data Protection Authorities, industry, and citizens. Clear rules are just as important as a uniform interpretation of those rules to ensure the trust of individuals and data subjects across the EU.

Transparency Register Number
52431421-12

1. **Anonymisation and means that can reasonably be used to identify the person**

The central point of the guidelines is that pseudonymised data, which can be linked back to an individual using additional information, is still considered personal data and we fully support this viewpoint.

However, according to relevant case law of the Court of Justice of the European Union (CJEU), we believe that the EDPB's Guidelines should reference and further develop the case law that establishes concrete criteria about which factors enters into play to consider reasonable means for reidentification. These criteria play a relevant role to decide when processed data would be pseudonymised data or anonymised data.

Specifically, Case Breyer (C-582/14) stated that there is no possibility of re-identification: *"when the identification of the data subject is prohibited by law or is practically unfeasible, for example, because it involves an excessive effort in terms of time, costs, and human resources, so that the risk of identification is actually negligible."*

Recently, in the Conclusions of the Advocate General Mr. Dean Spielmann regarding Case C-413/23, he recalls the conclusion of the General Court when it stated that: *"by not investigating whether Deloitte had the legal and practically feasible means to access the additional information necessary to re-identify the claimants, the SEPD could not conclude that the information transmitted to Deloitte constituted information about an "identifiable natural person" within the meaning of Article 3(1) of Regulation 2018/1725.*

It is also worth mentioning here Case C-479/22, where the interpretative elements applicable for determining the reasonableness of whether an organization can or cannot re-identify dissociated data are clarified: "*To determine whether there is a reasonable probability that means will be used to identify a natural person, all objective factors must be taken into account, according to Recital 16 of Regulation 2018/1725, such as the costs and time required for identification, considering both the technology available at the time of processing and technological advancements".*

It also incorporates a relative perspective on Case C319/22: *"the VIN constitutes personal data, within the meaning of Article 4(1) of the GDPR, of the natural person referred to in that certificate, in so far as the person who has access to it may have means enabling him to use it to identify the owner of the vehicle to which it relates or the person who may use that vehicle on a legal basis other than that of owner."*

We believe that the EDPB should actively promote a practical interpretation and consider the means that can reasonably be used to identify the person by both the controller and any other person not only because it aligns with the established case law of the Court of Justice of the European Union (CJEU), but also because it offers greater flexibility in the practical application of the regulation. By adopting this approach, the EDPB can ensure that the scope of pseudonymisation vs. anonymisation remains adaptable to the

evolving technological landscape, and ensures in practice at the same time the privacy and security of individuals.

Additionally, to implement this interpretation, we should refer to the principles outlined in the Data Governance Act (Recital 15), which clearly defines the conditions for data reuse, promoting the creation of secure processing environments that ensure the protection of privacy and the integrity of information. Within this framework, these environments are seen as an appropriate mechanism for the reuse of data, provided effective security measures are implemented. These secure environments can be both logical and physical, as well as organizational; logical separation significantly reduces costs and ensures better governance by avoiding organizational and/or physical silos. Such data would be considered non-personal data and appropriate for reuse if there is no reason to believe that the combination of different sets of data could lead to the identification of the data subjects. This rule also extends to pseudonymised data, ensuring that their processing complies with the established security and protection principles.

Also, the spirit behind the crafting of the GDPR was to strike a **balance between robust data protection and fostering of innovation**, ensuring that European businesses, especially in the rapidly evolving tech sector, could remain competitive on a global scale. An extensive interpretation of the concept of pseudonymisation versus anonymisation would not only undermine this balance but could also lead to a disadvantageous position for European companies, especially when compared to their counterparts in regions with more flexible data protection frameworks.

In this context, providing a favorable interpretation of pseudonymised data aligns with the initial intention of the Regulation: to **empower European companies to innovate responsibly, while maintaining a high standard of data protection**. Such an approach would reinforce **Europe's competitive position as a leader in both privacy and technological advancement.**

2. Pseudonymization as accelerator of Artificial Intelligence

Pseudonymization is crucial for data protection in the era of artificial intelligence (AI) and data-driven innovation. As part of Privacy-Enhancing Technologies (PETs), it helps balance data use with respect for individual rights. It allows data to remain useful while offering strong protection, supporting responsible AI development. We share this approach, recognizing the i**mportance of pseudonymization in fostering innovation without compromising privacy**.

We strongly believe that a very strict approach could lead to unintended consequences, like slow down the development of generative AI in Europe and reduce the innovation potential of AI in Europe, despite the continent's valuable data resources.

In its "European Data Strategy" from February 2020, the European Commission emphasized that "*data is vital for economic development*" and *"data availability is essential for training AI systems*." The Commission promised to use its influence to gather best practices for handling personal data, including pseudonymization. This aligns with our view that pseudonymization and anonymisation are essential in facilitating AI advancements while ensuring data privacy.

The AI Act also recognizes pseudonymization as a privacy protection measure. Article 10 states that providers of high-risk AI systems may process sensitive personal data if these data are protected with advanced measures like pseudonymization. This demonstrates how pseudonymization ensures both data utility and privacy protection in AI development, a principle we strongly support.

3. Implications for the rights of the data subjects

We welcome EDPB's efforts to ensure the protection of data subjects' rights. However, we believe that the obligation of identification in cases where the controller does not have the necessary attributes to identify could place an excessive burden on organizations.

In paragraph 78, it is stated that if the data subject can provide the pseudonym and prove that it belongs to them, the data controller would be able to identify them and, consequently, apply the data subject's rights. Furthermore, in paragraph 79, it is stated that the controller should include in the information required by Article 11.2 GDPR how the data subject can obtain the relevant pseudonym and how they can demonstrate their identity.

We believe this could result in an excessive burden and, at times, be difficult for companies to manage, as even though the user provides us with the attributes, in practice, it would be challenging to handle. It would involve a disproportionate effort both in terms of fulfilling the information obligation and in satisfying the data subject's rights.

4. Importance of data labelling

We agree with the benefits highlighted by the EDPB regarding pseudonymisation, but we believe that the importance of data labelling as a good practice has been overlooked. We would like to stress that data labeling is essential for pseudonymisation and effective auditing. In Telefónica we label all direct identifiers and quasi-identifiers of each "data entity", which allows for better control, auditing, and automation. This practice simplifies processes while ensuring data security.

5. Pseudonymisation for Compatible Purposes

Telefónica welcomes the EDPB's recognition of the application of pseudonymization for compatible purposes. If the Telco sector were subject to the same GDPR rules as other industries, pseudonymization could also play a critical role to foster innovation and competitiveness in the sector, provided GDPR's compatibility criteria of further data processing were applicable to traffic and location data. Unfortunately, so far telecom companies cannot benefit from Article 6 GDPR in general and, in particular, from Article 6.4. GDPR's approach, as it is not recognised in the outdated sector specific ePrivacy Directive (Directive 2002/58/EC).

Art. 6 GDPR, including compatibility through pseudonymization, could help process this data for a wide range of purposes that would benefit society as a whole, such as improving service quality and security, creating new personalized offerings, or conducting research to advance networks and technologies, all while protecting user privacy. It would also allow for collaboration among companies within the sector or with other partners, like tech service providers, without directly exposing personal data, thus fostering innovation and the development of new solutions.

We believe that the EDPB should (1) emphasize more the potential benefits of pseudonymization for compatible purposes, particularly in terms of creating new products and services, and more in particular, (2) reevaluate the strict interpretation that the EDPB makes of the outdated ePrivacy rules applicable to the processing of traffic and location data by the European telecommunication industry.

Adopting pseudonymization in this context can ensure better compliance with data protection regulations and simultaneously support the innovation and development of more personalized, cutting-edge products in telecommunications.

6. Clarification of Security Measures for Pseudonymised Data Processing

Telefónica believes it is necessary to more clearly specify the security measures that should be applied to the processing of pseudonymised data to minimize the risks of re-identification. It is crucial for the EDPB to establish guidelines on the use of appropriate techniques to ensure that pseudonymization is both effective and secure. This would enable greater protection of personal data while maintaining the balance with innovation and regulatory compliance.

7. Detailed Explanation of Key Concepts in the Guidelines

The guide introduces new concepts that, in order to be properly understood, require detailed explanations. A key example of this is terms like "pseudonymisation domain," "quasi-identifiers," or "pseudonymising controllers," which are mentioned without sufficiently clear definitions. To ensure that users and businesses can properly apply the

regulations, it is crucial that concepts like these be defined precisely and accompanied by practical examples.

8. **Clarifying the Difference: Pseudonymisation vs Anonymisation**

The Guidelines should provide a clearer and more detailed distinction between pseudonymisation and anonymisation. A stronger emphasis on this difference would help ensure that organisations and individuals applying these techniques can do so in compliance with data protection regulations, while also understanding the level of protection each method provides. Clear guidelines on anonymisation will support better decision-making in data processing practices and enhance trust in how personal data is handled.

Conclusions

Telefónica considers crucial to address how the means that can be used to identify the data subject could influence the determination of whether data should be considered pseudonymised or anonymised adopting a more subjective interpretation of reasonable means. Such an approach would help promote innovation and allow companies to develop new services, all while maintaining a strong commitment to data protection. By encouraging this flexibility, businesses can better balance the need for privacy with their goals for growth and technological advancement.

Furthermore, the guidelines should provide more detailed explanations of new concepts and the security measures related to pseudonymisation. This would not only make it easier for companies to comply with regulations but would also empower them to utilize pseudonymisation effectively as a tool for creating safer, innovative products and services. We encourage the EDPB to take these considerations into account and to refine the guidelines with clear, practical guidance that fosters both compliance and innovation.

14 March 2025