SAMMAN

Comments on the EDPB draft guidelines 01/2025 on pseudonymization adopted on January 16th, 2025

14 mars 2025

SAMMAN Law and Corporate Affairs firm welcomes the publication of the Draft Guidelines 01/2025 on Pseudonymization by the European Data Protection Board (**EDPB**). These guidelines have the potential to enhance the understanding of pseudonymization as a key privacy protection technique under the General Data Protection Regulation (**GDPR**) and could foster privacy-by-design approaches across sectors.

In response to the EDPB consultation, SAMMAN wishes to contribute by sharing a study on pseudonymization published in September 2024 (**1**) and short comments on the Draft Guidelines (**2**).

1. Key take aways from the Study on the Importance of Pseudonymization in the Age of Artificial Intelligence

Given the technical and legal ambiguities surrounding this technique, SAMMAN commissioned a study on "The Importance of Pseudonymization in the Age of Artificial Intelligence: Beyond the Binary" (in French) by Théodore Christakis, Professor of international and European law at the University of Grenoble Alpes and Director of the Center for International Security and European Law (CESICE).

The study highlights the crucial role of pseudonymization in GDPR compliance. The GDPR mentions pseudonymization 15 times as a measure to:

- Reduce the risk that processing poses to the rights of individuals (Recital 28);
- Strengthen the security of personal data (Article 32);
- Ensure data protection by design (Article 25);
- Promote compliance with several cardinal data protection principles, such as the principle of data minimization (Article 25), storage limitation (Article 5(1e)), purpose limitation (5(1b)), and the security obligation (5(1f)).

The GDPR also calls for the establishment of codes of conduct on pseudonymization in Article 40(2).

Moreover, the study shows that pseudonymization is widely endorsed by European institutions, such as the European Union Agency for Network and Information Security (**ENISA**), as an effective technique to facilitate the processing of personal data while providing solid protection guarantees.

Yet, despite its widely recognized benefits, implementing pseudonymization techniques faces legal uncertainties. The study outlines two diverging approaches regarding pseudonymisation:

- The **"relative"** approach, which considers t whether re-identification is realistically possible in a given context, and
- The **"absolute"** approach, which assumes that any theoretical possibility of re-identification is sufficient to classify data as personal.

The study proposes to go beyond this binary framework and consider pseudonymization as an essential component of data management strategies. Indeed, pseudonymization can be a pragmatic solution to facilitate secure data sharing, for instance within common European data spaces, especially in the field of health, and for the responsible development of AI.

The study concludes that "*a very strict approach that does not fully take into account robust pseudonymization mechanisms will have undesirable consequences*", in particular for scientific research and the development of generative AI in Europe.

2. Considering the aspects outlined in the study, we recommend to:

- **Clarify the distinction between pseudonymization and anonymization**

The Draft Guidelines outline very high requirements for considering data as pseudonymized, making it nearly equivalent to anonymization. By requiring data controllers to ensure that no party can re-identify the data - a criterion for anonymization - the guidelines risk creating legal uncertainty. The GDPR makes a clear distinction between these concepts: pseudonymization aims to make identification difficult, while anonymization makes it impossible.

- **Adopt a balanced approach to personal data classification**

The Draft Guidelines take an absolute approach, proposing a strict definition of pseudonymization. It considers that the mere theoretical possibility of re-identification is sufficient to classify data as personal. However, Recital 26 of the GDPR states that the possibility of re-identification must be realistically assessed, taking into account the means that "*are reasonably likely to be used to identify a natural person*" such as the costs incurred, the time required, and the technologies available.

- **Take into consideration existing use cases and pseudonymization compliance tools**

The examples provided in the Draft Guidelines mainly concern the health sector and the processing of sensitive data. This limitation does not reflect the diversity of use cases for pseudonymization in the digital economy meeting very diverse needs (e.g., data analysis, training of AI algorithms, advertising and marketing, etc.).

The final Guideline should also include references to international standards (such as ISO/IEC 20889:2018 and ISO/IEC 27559:2022) that help companies implement standardized pseudonymization solutions.

- **Adjust the guidelines to prevent potential contradictions with future case law**

The guidelines are being finalized while a crucial case is pending before the Court of Justice of the European Union (**CJEU**). The case *EDPS vs. SRB (C-413/23 P)*, between the Single Resolution Board (**SRB**) and the European Data Protection Supervisor (**EDPS**), concerns precisely the debate between the "relative" and "absolute" approaches to personal data and their impact on the definition of pseudonymized data. The outcome of this case could change the current interpretation of the law.

Advocate General Dean Spielmann presented his conclusions on February 6th, 2025. He supported the approach taken in the first instance, before the European General Court (**EGC**), which had ruled in favor of the SRB. He reiterated that anonymous data is excluded from the scope of the GDPR, while pseudonymized data remains subject to the GDPR if the data subjects are identifiable. However, he considered that pseudonymized data may escape the qualification of personal data if the risk of identification is non-existent or insignificant. Thus, if the recipient of the data cannot reasonably identify the data subjects, such data should not be considered personal data in relation to him or her.

In order to avoid legal uncertainty for companies, it would be preferable to wait for the outcome of the ongoing court case before publishing the final guidelines, or to adopt a more cautious and balanced approach.

*　　*
*