Public Consultation

Guidelines 01/2025 On Pseudonymisation

Adopted On 16 January 2025

I. Introduction

MyData-TRUST is a company registered under Belgian Laws, active since 2017 in the data protection area. Its multi-disciplinary team includes Data Privacy Lawyers, IT Security Specialists and Clinical Experts providing GDPR related services (such as privacy risk assessments, external DPO as a service, etc.). Our clients include among others Pharmaceutical, Biotech and Medical Devices companies, Contract Research Organisations (CROs), Healthcare providers and associations.

II. Key Messages

MyData-TRUST (hereinafter "MDT") salutes the recent adoption of the guidelines 01/2025 on pseudonymisation (hereinafter "the Guidelines") and would like to draw the attention of the European Data Protection Board (EDPB) on a few points summarised below and further discussed in the following pages. These points concern the application of the Guidelines to life sciences. MDT recommends:

- To add an advice to use a assessment methodology with a measurable re-identification score to classify datasets as either pseudonymised or anonymised (III.A.).
- To explore the inclusion of examples of modern pseudonymisation techniques, such as tokenisation, in the guidelines (III.B.).
- To assess the possibility of the extending the provisions of GDPR Article 11 to the provision of information in case of pseudonymised data where the data controller does not have access to additional information (III.C.).
- To exclude means that violate third-country legal norms by public authorities from the assessment of pseudonymisation effectiveness in Transfer Impact Assessments (III.D.).

- To promote the deployment of general information platforms such as Europe-wide transparency portals applicable to scenario where the Controller receives pseudonymised data (III.D.).

III. Detailed Contribution

A. Reidentification Risk Assessment and Evaluation

The executive summary of the guidelines reaffirms that pseudonymised data remains personal data subject to the GDPR. However, this statement does not sufficiently capture the evolving nature of pseudonymisation techniques and their varying degrees of effectiveness.

Instead of treating pseudonymised data as inherently subject to the GDPR, the analysis should adopt a risk-based approach, considering the likelihood and feasibility of re-identification. Different pseudonymised datasets should not therefore be considered as a uniform category but rather as existing on a continuum between identified data and anonymous data, considering a whole diversity of richness of information. Depending on the context, the richness of the data and the number of individuals, some pseudonymisation techniques can be considered as sufficiently effective for anonymity. For example, a dataset of four rare disease patients in a single region carries a higher re-identification risk compared to a dataset of over 500,000 flu patients across multiple countries, even when using the same pseudonymisation method.

The guidelines currently lack practical criteria to differentiate between effectively pseudonymised data to simply prevent data subject identification and data that is so well deidentified that it is closer to anonymisation. To address this, MDT proposes introducing **the concept of identifiability continuum,** recognizing that pseudonymisation techniques can reduce re-identification risks to a level where data is functionally anonymised within a pseudonymised domain. This assessment should take into account the context, the reasonable means available for re-identification, and the security of the key.

To operationalize this approach, **MDT suggests** that the EDPB promote the adoption of a risk-based methodology to assess re-identification potential, resulting in a measurable score that classifies datasets as lowly-pseudonymised, highly pseudonymised, or anonymised before processing begins.

This structured classification would enhance legal clarity and improve the practical application of pseudonymisation techniques in compliance with the GDPR.

B. Focus On Modern Pseudonymisation Techniques

These guidelines primarily focus on traditional pseudonymisation techniques such as cryptographic one-way functions, encryption, and lookup tables. However, tokenisation is also a noteworthy security measure for protecting sensitive data (e.g. credit card number in banking or data subject identification in clinical trials). This technique is to replace and exchange a valuable item with a secured, symbolic and non-sensitive token that holds no intrinsic value. The original sensitive data is substituted with a random string of characters (the token); which has no usable value outside the secure system where it can be reconverted. To establish the unique link between the token and the original data, algorithms are used, with the link stored in a secured environment.

Unlike anonymisation but similar to pseudonymisation, tokenisation is reversible and can therefore be considered a pseudonymisation method. It ensures that even if "digital or real pickpockets" steal the token, it remains useless without access to the key needed for decryption - much like stealing a concert ticket receipt without the actual ticket. This perspective aligns with ISO/IEC 20889:2018 and PCI DSS Tokenisation Guidelines.

MDT highlights the lack of substantial discussion on more recent technologies in the guidelines and **requests** explicit reference to tokenisation as an important pseudonymisation technique.

C. Impact of Pseudonymisation on the Obligation to Inform Data Subjects

MDT recognizes that effective pseudonymisation is a key data protection technique under the GDPR, significantly reducing the risks associated with personal data processing. While the guidelines explicitly state that the processing a pseudonymised dataset may justify, under certain conditions, the non-application of data subject rights listed in Articles 15 to 22, they fail to address how pseudonymisation affects the controller's obligation to provide information under Articles 14 and 11(2) GDPR.

In the context of scientific research, the very purpose of pseudonymisation is for the researcher (Controller) to avoid having any contact with data subjects enrolled in the study. This aligns with Article 11(1) GDPR, which allows Controllers not to collect identifying data when the purposes of processing do not require identification.

Requiring the Controller to comply with Article 11(2) contradicts Article 11 (1), particularly when the Controller cannot rely on the exception under Article 14 (5)(b) (i.e., when providing information is impossible or requires disproportionate effort). Informing data subjects would often necessitate their identification, which the Controller is actively seeking to avoid. This requirement also contradicts the principle of data minimisation, as it would force the Controller to engage in unnecessary additional processing. Even more concerning, the guidelines suggest that Controllers inform data subjects about the entity holding additional information necessary for re-identification – which undermines the very purpose of pseudonymisation

MDT suggests that the EDPB:

- Clarify when a controller receives pseudonymised data in a way that prevents re-identification under the conditions set out in these guidelines, the obligation to provide specific information leading to reidentify the data subjects should be waived or assigned to the entity responsible for pseudonymising the personal data.
- Promote the creation of general information platforms, such as Europe-wide transparency portals, to facilitate compliance with information obligations in a practical and scalable manner.

D. Evaluation of Pseudonymisation as a Supplementary Measure

MDT acknowledges and appreciates the EDPB's considerations on the use of pseudonymisation as an effective measure for data protection by design and by default, as well as a supplementary measure for third country data transfers to ensure compliance with GDPR, Articles 44 and 46(1).

However, the conditions outlined in paragraph 64 of the guidelines for the effective use of pseudonymisation in transfers, may be challenging for data exporters to meet in practice. If the unlawful means available to third country authorities to access additional data are considered, no pseudonymisation measure could ever be deemed fully effective. MDT strengthens this stance with two key arguments:

- Given the extent of the resources (lawful or otherwise) that third country authorities may have at their disposal – and the fact that these resources are rarely publicly documented – a Controller can hardly guarantee that any pseudonymisation measure meets the standard set out in paragraph 47 of the guidelines.
- Additionally, during the pseudonymisation process, it may be difficult for the pseudonymising Controller to assess whether third country public authorities could obtain the necessary additional information to re-identify data subjects. Such access means may not be publicly known, particularly if obtained outside a national legal framework.

These factors make the threshold for pseudonymisation as a supplementary measure in data transfers particularly difficult to achieve.

MDT therefore suggests that the EDPB excludes the reference to public authorities' reasonable efforts that may infringe third-country legal norms from the elements that must be mandatorily considered when securing the pseudonymisation domain.