EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

14 March 2025
EMA/75472/2025
European Medicines Agency

Response of the European Medicines Agency to the European Data Protection Board's Public Consultation on Guidelines 01/2025 on Pseudonymisation

The European Medicines Agency (EMA) welcomes the European Data Protection Board (EDPB) Guidelines 01/2025 on Pseudonymisation (the 'Guidelines') and appreciates the opportunity to comment on the draft guidelines in the course of the related public consultation.[1]

EMA commends the EDPB's work to strengthen regulatory clarity on data protection principles and complex practical matters, such as pseudonymisation. The Guidelines are particularly welcomed as they offer clarification on key definitions and principles, and practical guidance, along with examples, to assist data controllers in effectively implementing pseudonymisation. In particular, the clarification of the conditions required for pseudonymisation to serve as an effective supplementary measure for transfers to third countries is highly valuable, as are the explanations regarding the rights of data subjects in relation to pseudonymised data that may pertain to them.

To contribute to the Public Consultation, EMA has identified several areas where additional clarification or practical guidance would be welcome - as presented in the table below.

Reference	Comment
General comment, Executive Summary	A summary of key takeaways could aid in the comprehension of individuals without pseudonymisation expertise.
General comment, Executive Summary and Paragraph 22	In relation to the distinction between pseudonymisation versus anonymisation, the Guidelines merely state that pseudonymised data can be considered anonymous only if the conditions for anonymity are met. It would be beneficial to provide further clarification on what constitutes the conditions for anonymity. In particular, the EDPB could address whether the

[1] Guidelines 01/2025 on Pseudonymisation | European Data Protection Board

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

Reference	Comment
	Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques remains applicable. Additionally, references to relevant case law from the Court of Justice of the European Union (CJEU) addressing the conditions for anonymity could enhance the Guidelines. Notably, cases such as *Breyer (C-582/14)* and *EDPS v SRB (C-413/23 P)* could enrich the Guidelines on the nuances of pseudonymisation versus anonymisation. While the latter case is still pending, the judgment anticipated in the coming months holds the potential to offer critical interpretive guidance on this very distinction.
General comment, Paragraph 13	Paragraph 13 of the Guidelines on Pseudonymisation refer to the following: "*It is important to look beyond the confines of the organisation of a single controller pseudonymising data. Personal data is frequently pseudonymised before it is shared with other controllers or to processors to limit the risks involved in that sharing. Pseudonymised data coming from different controllers might need to be brought together and linked. Or, in contrast different data sets need to be pseudonymised in a way that assures that they cannot be linked*". This is an important statement reflecting real word scenarios such as the medicines regulatory and safety monitoring domain. It would be of added value to further elaborate on how best to approach pseudonymisation of already pseudonymised data for further processing (e.g. scientific research) based on the already described pseudonymisation techniques and the need to maintain data utility. Explanations (examples) on suitable pseudonymisation techniques and additional organisational measures that could minimise the risk of linkage of data sets that could lead to potential re-identifications of data subjects would be particularly helpful (e.g. in the area of adverse reaction reporting and pharmacovigilance).
Paragraph 18	Paragraph 18 states that: '*The pseudonymising transformation may and regularly does replace part of the original data with one or several pseudonyms—new identifiers that can be attributed to data subjects only using additional information.*' For the sake of clarity, it would be helpful to refer to direct identifiers instead of 'part of the original data'. The proposed wording would therefore read as follows: '*The pseudonymising transformation may and regularly does replace the direct identifiers with one or several pseudonyms—new identifiers that can be attributed to data subjects only using additional information.*'
Paragraph 21	Paragraph 21 suggests that additional information could be understood as any data or information beyond the immediate control of the pseudonymising controller or processor (e.g. information from publicly accessible sources like posts in a social media or an online forum). This seems to be at odds with the second part of the pseudonymisation definition given in Article 4(5) of the GDPR "*…provided that such additional information is kept separately and is subject to*

Reference	Comment
	technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." In addition, Recital 26 of the GDPR explains that it is when determining whether a natural person is identifiable that account should be taken of all the means reasonably likely to be used, also by another person, to identify the natural person directly or indirectly. Accordingly, it would be recommended to clarify that publicly available sources may need to be considered as means reasonable likely to be used for identification (attribution), but they are not part of the additional information within the control by the pseudonymising controller.
Examples of pseudonymisation techniques	Whilst the description of the practical use of cryptographic algorithms and lookup tables are much appreciated, further explanations/examples on other emerging privacy enhancing technologies could be beneficial e.g., use of differential privacy or homomorphic encryption acknowledging that they are not typically considered as pseudonymisation techniques.

EMA would appreciate if these aspects could be addressed by the final Guidelines. Thank you for taking our comments into considerations. We remain available should you need any clarifications regarding the above.