HDL

Federal Institute for Drugs and Medical Devices

Health Data Lab (Federal Institute for Drugs and Medical Devices, Germany)

Public Consultation European Data Protection Board: Guidelines 01/2025 on Pseudonymisation (Commentary)

Version 01-00-000

Health Data Lab (Federal Institute for Drugs and Medical Devices, Germany)

Table of Contents

Health Data Lab (Federal Institute for Drugs and Medical Devices, Germany)

Public Consultation European Data Protection Board: Guidelines 01/2025 on Pseudonymisation (Commentary)

1 No. 21

1.1 Text of No. 21

Additional information may also exist beyond the immediate control of the pseudonymising controller or processor. The pseudonymising controller or processor should take such information into account in the assessment of the effectiveness of pseudonymisation to the extent such information can reasonably be expected to be available. For example, information from publicly accessible sources, such as posts in a social media or an online forum, may contribute to the attribution of pseudonymised data to data subjects. This assessment will help determine if any further measures need to be implemented to avoid attribution.

1.2 Proposal for insertion after No. 21

An assessment of all available information from accessible sources on a very detailed level (for instance, evaluation of all social media posts on every social media platform) is neither necessary nor feasible. The assessment should be limited to a theoretical evaluation.

1.3 Reasoning

It is sufficient for the pseudonymizing controller or processor to know what type of information may theoretically be available from other sources. It is not necessary and usually not realistic to analyse all publicly available information.

2 No. 77

2.1 Text of No. 77

Art. 11 GDPR recognises that the controller may be able to demonstrate that it is not in a position to identify the data subject, including in pseudonymised data it holds. This may be the case if the controller does not have (or no longer has) access to additional information allowing attribution, is demonstrably unable to lawfully obtain such information and is demonstrably unable to reverse the pseudonymisation with the assistance of another controller. Consequently, except where the data subject (for exercising his or her rights) provides additional information enabling his or her identification, the rights of the data subjects enumerated in Art. 11(2) or 12(2) GDPR, respectively, shall not apply in this case. In compliance with Art. 11(2) GDPR, the controller has to inform the data subject accordingly, if possible.

2.2 Proposal for the replacement of No. 77

Art. 11 GDPR recognises that the controller may be able to demonstrate that it is not in a position to identify the data subject, including in pseudonymised data it holds. This may be the case if the controller does not have (or no longer has) access to additional information allowing attribution, is demonstrably unable to lawfully obtain such information and is demonstrably unable to reverse the pseudonymisation **without** the assistance of another controller. Consequently, except where the data subject (for exercising his or her rights) provides additional information enabling his or her identification, the rights of the data subjects enumerated in Art. 11(2) or 12(2) GDPR, respectively, shall not apply in this case. In compliance with Art. 11(2) GDPR, the controller has to inform the data subject accordingly, if possible.

2.3 Reasoning:

The controller should be able to show that they alone are not able to reverse the pseudonymisation. Reversal may be possible with the help of another controller.

Health Data Lab (Federal Institute for Drugs and Medical Devices, Germany)

3 No. 78

3.1 Text of No. 78

For instance, if the data subject can provide the pseudonym or pseudonyms under which data relating to them is stored, and proof that those pseudonyms pertain to them, the controller should be able to identify the data subjects. In consequence, the data subject rights should apply in this case.

3.2 Proposal for insertion after No. 78

A controller may only disclose pseudonymised personal data to a data subject, if the controller can – without the help of another controller – authenticate the relationship between data subject and the pseudonym claimed by the data subject to be his/her pseudonym with a level of certainty appropriate in relation to the sensitivity of the data. If such an appropriate level of authentication cannot be achieved, the controller may not disclose any personal data to the person requesting this data.

For example, if an online-advertising platform generates a unique ID stored in a data subject's browser, the data subject could request the advertising profile (interests etc.) stored on the platform's server for the generated ID in a cookie in the data subject's browser. The online-advertising platform could simply provide a website that receives the cookie with ID and provided a web page with functions supporting the data subject's rights (transparency, deletion, change etc.). The fact the data subject has access to the browser with the ID (pseudonym) in a cookie could be regarded as an appropriate level of authentication to disclose the interest profile generated by interactions from this browser.

However, a data centre storing the pseudonymised medical history of data subjects based on a pseudonym created by another controller (the trust centre) cannot – on its own – authenticate a data subject with an appropriate level of certainty for highly sensitive medical data. The authentication could only be based on parts of the medical history of a data subject, which might be known to or can be obtained with some effort by a malicious third party. Therefore, a data centre storing sensitive pseudonymized information based on pseudonymisation by another controller typically may not disclose any pseudonymized sensitive information to data subjects.

The provision described in Article 11 (2) sentence 2 of the GDPR, which requires controllers to identify data subjects using additional information provided by the data subject, should not apply where this jeopardises the protection associated with the procedure and another controller can readily provide the requested information. In such cases, the controller should only be obliged to inform data subjects of this possibility and to direct them to the other controller.

3.3 Reasoning

In the view of the Health Data Lab, this data subject right against the controller is dispensable here. Data subjects can obtain exactly the same information directly from the insurer (as another controller) without the need to reverse the pseudonymisation or jeopardise the procedure.