Spolek pro ochranu osobních údajů

Comments on the EDPB's draft "Guidelines 01/2025 on Pseudonymisation"

We welcome the opportunity to provide feedback on the recently published EDPB draft Guidelines 01/2025 on Pseudonymisation ("Guidelines").

We greatly appreciate the EDPB for preparing these Guidelines addressing a very important question concerning the protection of personal data.

General Comments

We believe that the question of pseudonymisation is closely related to the definition of personal data, and in particular to its relative concept, as declared in the CJEU judgments Breyer (C-582/14) and Scania (C-319/22) and more recently in the Advocate General's opinion in Case C-413/23 P. It would therefore be prudent to examine more closely the question of the identifiability of individuals from the pseudonymised data from the perspective of the person who processes such data. If the Guidelines' envisaged scope does not allow to address the question of the definition of personal data in detail and in accordance with the current case-law, it would be preferable to limit the scope of the guidelines to a purely technical assessment and exclude the sections directly related to the definition of personal data aside.

From this perspective, we consider the following conclusions from the executive summary to be at least partially simplistic: *„Pseudonymised data, which could be attributed to a natural person by the use of additional information, is to be considered information on an identifiable natural person,[2] and is therefore personal. This statement also holds true if pseudonymised data and additional information are not in the hands of the same person."* Unless the person who will have access to the data in question is able to link the data to a specific person using reasonable legal means, the data will be anonymous from their perspective (relative concept of personal data) and therefore not personal data.

Similarly, we do not believe that the mere possibility of illegal access to data (e.g. by cyber-crime actors) and subsequent potential of linking it to other data (as de facto outlined in points 38, 42 and 60 of the Guidelines) should lead to a conclusion that pseudonymous data is always personal data including for the person with access only to a legally available pseudonymised portion of the dataset. See also the conclusions of the CJEU in the Breyer case regarding the concept of personal data and the presumption that the person concerned has access to legal means which enable them to identify the data subject. While we concur that attempts to obtain data illegally must also be taken into account for the purposes of implementing appropriate security measures, it is essential to maintain a nuanced understanding of the implications of overly broad definitions of personal and pseudonymous data. It cannot be reasonably expected from controllers or processors to consider such illegal activities or criminal intents that go beyond the state-of-the-art security practices and measures while assessing their pseudonymization processes.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

Similar oversimplification can be found in point 93 of the Guidelines: *„Lookup tables are personal data since they allow the identification of data subjects."* We would like to point out that for some lookup datasets (especially if it is not clear in what context they were collected and by which controller), even the inclusion of a person's name with (and only with) an identifier number (as the only other data) may not be considered personal data, especially for persons who, following the above relative concept of personal data, will not be capable of any additional identification (or association with other data) and cannot dispose with second part of the database.

In fact, in our view, the following questions may play a significant role here, in addition to the facts mentioned in the Guidelines:

1) Whether the person who possesses or processes (only) the pseudonymized dataset is acting as (i) a processor or joint controller with the person who performed the pseudonymization or is acting as (ii) a fully independent person (separate data controller). Specifically, it is crucial to determine whether the processing of the pseudonymised dataset is part of a single processing activity (albeit a broader one) or whether it is a completely independent processing.
2) Whether it is apparent to the person in possession of the (only) pseudonymised dataset, or was known to him/her, that the dataset contains personal data in pseudonymised form (which may not always be obvious)
3) Whether or not the pseudonymised data have been made public (see also the conclusions of the OLAF judgment of CJEU, C-479/22).[1]
4) Whether there is a risk that the data subject can be directly or indirectly identified only on the basis of the data contained in the dataset itself (e.g. as a result of 'singling out') without compromising the separate database (lookup tables) itself containing directly identifying data (see also points 47 and 64 of the Guidelines in this respect).

Additionally, we would appreciate the inclusion of examples in the Guidelines of the categories of types of data that in practice are often (incorrectly) considered as pseudonymised (even though the pseudonymisation process in the strict sense was not applied to them), such as (most) data obtained through cookies and similar technical tools.

Specific Comments

Point 51 of the Guidelines:

Point 51 of the Guidelines stipulates that: "*In particular, all intended recipients of the pseudonymised data need to demonstrably assure that the pseudonymised data are not disclosed to unauthorised recipients beyond the defined domain*". We believe that no specific assurance or declaration to this effect is necessary, particularly for processors. The general principles of Article 28 of the GDPR or, for recipients who are independent or joint controllers, a general obligation to process data in accordance with the GDPR and other regulations apply directly.

Point 54

Regarding point 54 and the opinion that: *„Specific EU or Member State law may require certain data to be pseudonymised as a condition for the lawfulness of its processing, thus making*

[1] For this case, it might then be appropriate to consider applying a test similar to the "motivated intruder" test as formulated by the UK ICO.

pseudonymisation an obligatory measure to meet the lawfulness principle.", we would recommend a more balanced expression in this matter. A requirement to perform pseudonymisation may be justified in the context of e.g. sectoral regulations, but it is also conceivable that a Member State may impose this requirement as a general requirement on certain categories of data. In such a case, however, the motivation or consequence of such a requirement might not be the interest in the protection of personal data, but the interest in favouring controllers and processors established in that Member State, since controllers and processors from Member States where such a requirement would not be universally applied would have to incur additional costs for such processing (e.g. to adapt their IT systems, etc.). Such a requirement could then be contrary to the principle of free movement of personal data within the meaning of Article 1(3) GDPR.

Point 61

Point 61 states: *„The security level reached with the help of pseudonymisation depends on the security level achieved for both pseudonymised and the relevant additional information. If it is easy for an unauthorised actor to obtain the relevant additional information, then the security benefit of pseudonymisation is small, and might well be negligible or lost."* We believe that this conclusion could be (mis)interpreted as overly strict. Superior protection of at least one of the two datasets (while maintaining a reasonable level of protection for the other dataset) can significantly increase the overall level of data security, which is after all the usual goal of pseudonymisation.

Point 63 and 64

Points 63 and 64 of the draft guidelines state that the use of pseudonymisation may be considered as a supplementary measure when transferring data outside the EU/EEA on condition, inter alia (point 63), that: *„the authorities are not able to single out a data subject in the course of an interaction with members of a group of persons based on the pseudonymised data and information they are able to obtain with reasonable effort."* We kindly ask for clarification on the EDPB's perspective on the security implications of such authorities being able to single out specific individuals in a dataset, but only in exceptional circumstances on the side of a particular person (e.g. data can only be obtained if the person in the dataset visits that third country, which of course cannot be assumed for all of persons).

Point 65

Point 65 states: *"Thus, any design of a pseudonymisation procedure needs to start from an assessment of which information the public authorities of the recipient country can be expected to possess or to be able to obtain with reasonable means, even if those means may infringe the legal norms in the third country. This information must then be assumed to be available in the pseudonymisation domain."*

We respectfully disagree with the requirement to consider illegal activities on the side of the public authorities. Expecting public authorities to behave illegally clearly defies any reasonableness and makes any assessments virtually impossible.

Point 77

Point 77 of the Guidelines interprets quite broadly the obligation of the controller to try to re-identify data subjects as well: *„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." We do not believe that the controller is obliged to attempt to obtain additional information that would allow re-identification of the data subject from a third party unless the controller is able to obtain such data from its processor or joint controller. We kindly ask for clarification on the legal basis for processing on the third party's side in case such third party was supposed to provide the data to the controller without a direct request from the relevant data subject. Note that such data may often be subject to confidentiality and professional secrecy.

Point 98

Point 98 states: *„For purposes that do not require linkage of records, data protection by design calls for the removal of individuals' "long term" identifiers (e.g. a "health service ID") while replacing transactional or "short term" identifiers (e.g. a "case number") by pseudonyms."* In our view, this is a somewhat categorical conclusion. We do not believe that Article 25 GDPR implies such an obligation.

Point 101

In point 101, it would be beneficial to outline the level of efforts the EDPB anticipates in regard to persons who would potentially perform the combination in question that would result in these attributes qualifying as quasi-identifiers *(„If a combination of those attributes are sufficient to attribute at least part of the pseudonymised data to data subjects, then they are called quasi-identifiers"*.)

Point 110

Regarding point 110, it would be beneficial to add a few specific examples of how the EDPB envisages such technical measures being implemented when, as correctly stated, "*Since controllers usually do not have control over the devices...*". Indeed, pseudonymisation itself is usually chosen by the controller as an additional security measure and should be sufficient on its own.

Point 116

We respectfully disagree with the conclusion expressed in paragraph 116 that: *„Correspondingly, this type of pseudonymisation may not significantly reduce the severity of risks associated with unlawful or unauthorised disclosure of the pseudonymised data."* We consider that the nature of the data and the real possibility of re-identification is also relevant and must be taken into account within the risk assessment. Additionally, it is not clear on what basis this conclusion was made: „*The use of such pseudonymisation is admissible if and only if the linking of different pieces of pseudonymised data relating to the same person may become necessary and will be lawful in this case*."

We appreciate the provision of specific examples in the annex. The majority of them are clear and will be helpful in our practice. However, we do not consider some of them to be entirely appropriate and consistent with real practice. It would be beneficial to clarify that the EDPB does not consider these examples as cases where pseudonymisation should be mandatory.

In Example 1, it is not clear to us from the whole context why the "user id" should be pseudonymised, or whether this is really such an essential measure, especially if the processing is carried out within a single company. In these cases, we consider the pseudonymisation of the user id to be somewhat superfluous.

Similarly, in Example 2, we do not consider it necessary to introduce pseudonymisation in the case of such processing by a mere organisational unit of the controller concerned.

In Example 7, we do not consider it realistic that in the case of a data breach, there will always be additional pseudonymisation of logs in the event of a transmission to the CSIRT team, especially after IP addresses and 'login credentials' have been removed as part of the initial pseudonymisation process. It is important to note that in many cases, prompt action needs to be taken and putting the controller concerned at risk of not performing the degree of anonymisation required by the EDPB could ultimately lead to the reluctance to perform any forensic analysis of the data.

In Example 8, we observe that in these cases, pseudonymisation is not typically used in practise. We believe that it is not necessary to pseudonymise such data in order to constitute compatible purposes.

We are grateful for the opportunity to provide our comments on the draft Guidelines. We would like to thank the EDPB very much for its efforts to clarify various issues related to the processing of personal data. We hope that our comments will help in formulating the final version of the guidelines.

Prague, 27.2.2025

JUDr. Vladan Rámiš, Ph.D.
Chairman of the Committee
Spolek pro ochranu osobních údajů

Mgr. František Nonnemann
Vice-Chairman of the Committee
Spolek pro ochranu osobních údajů

Mgr. Ing. Jakub Hruška
Spolek pro ochranu osobních údajů