VIDEOGAMESEUROPE

Public Consultation on the EDPB's Guidelines 01/2025 on Pseudonymisation

Response from VIDEO GAMES EUROPE

Transparency Register Identification Number: 20586492362-11

1. Video Games Europe welcomes the opportunity to provide comments on the pseudonymisation guidelines issued by the European Data Protection Board (EDPB). Our members welcome the issue of Guidelines and Recommendations by the EDPB as they promote a common understanding of the European data protection framework and provide a harmonised interpretation of key provisions in the GDPR. This will help to ensure an effective and meaningful implementation of the GPDR.

2. Overall, we believe that these Guidelines are overly abstract and introduce numerous new concepts that are not part of the existing EU legal framework. Although we appreciate the inclusion of examples in the Annex, we believe that the Guidelines should focus more on offering practical guidance and best practices for effectively applying the concept of pseudonymisation in accordance with GDPR legal obligations, instead of creating an entirely new conceptual framework.

3. The introduction of new concepts like pseudonymisation domain, pseudonymisation secrets, and quasi-identifiers raise concerns regarding their clarity and applicability in real-world business settings. In an environment where data processing is becoming increasingly multifaceted due to the proliferation of controllers, processors, and third-party entities, these terms are abstract and challenging to implement effectively. Although we recognise that these concepts are intended to provide guidance, they are not enshrined in the GDPR and should not therefore have any legal bearing. It would be helpful to have this clarified in the Guidelines.

4. We will highlight our comments following the order of the table of contents and corresponding paragraph numbers. The most important points that we wish to make are:
    - Pseudonymous data can legally escape the classification of personal data if no "reasonable means" for identification are available and the risk of identification is non-existent or insignificant.
    - The crucial role that contractual agreements can play in preventing the attribution of data to a natural person should be recognised in the context of defining pseudonymous data. Their role must be considered as part of the assessment of whether any "reasonable means" for identification are available.

- Previously obtained consent is a sufficient legal basis for the purposes of applying the pseudonymising transformation in cases where consent is the legal basis for the processing of the personal data.
- Data controllers will not be able to anticipate which persons may attempt to gain access to the data illegitimately, which causes tension with the clear recommendation in the Guidelines not to share pseudonymised data beyond the domain, i.e. the clearly defined group. Controllers should not be put in such an untenable position, nor any position that requires them to incriminate persons in this regard.
- When defining the conditions for handling pseudonymised data, the Guidelines must recognise the difference between the mere technical ability to reconstitute pseudonymised data as opposed to the ability to have the necessary access and authorisation to perform this operation.
- When pseudonymisation is used as a "supplementary measure" for the transfer of personal data, data controllers should not be required to consider practices that lie outside the legal framework of the recipient country or that go beyond what can reasonably be expected from supplementary measures under the GDPR.
- It should be clearly stated in the Guidelines that pseudonymised data cannot be considered personal data for a controller if the controller does not have "means reasonably likely to be used" for identification and is demonstrably unable to identify the data subject.
- The recommendation to provide the identity and the contact details of the source of the pseudonymised data in cases where the controller is required to inform the data subject that re-identification of the pseudonymised data is not possible, may increase the risk of unauthorised or unlawful processing and accidental loss of the pseudonymised data. This requirement conflicts with the requirement to ensure the security and protection of the processing of personal data by using appropriate technical and organisational measures and could result in risks to the fundamental rights and freedoms of the data subjects.

Detailed analysis

2.1 Legal definition of pseudonymisation

5. The Guidelines identify in §22 pseudonymised data as information on an identifiable natural person and therefore as personal data. They then state that this is also the case when "*pseudonymised data and additional information are not in the hands of one person and could be combined having regard to the means reasonably likely to be used by the controller or by another person*". However, as stated in the recently published Opinion of the EU Court of Justice's Advocate General Spielmann in the **EDPS vs. SRB case** (Case C-413/23 P), pseudonymous data can legally escape the classification of

personal data if no "reasonable means" for identification are available and the risk of identification is non-existent or insignificant (see §57 and §59 of the Opinion). While the CJEU decision on this case is still pending, Video Games Europe cautions against stating that pseudonymised data is still personal data even when the risk of identification is insignificant or non-existent, as it will cause legal uncertainty. Moreover, we suggest that the Guidelines should also analyse their interpretation of the definition of pseudonymisation in the context of all relevant CJEU case law (Breyer, Scania, IAB Europe).

6. The Guidelines should address whether parties can use additional measures (contractual, security over source data, etc…) to enable the receiving party to demonstrate that data is anonymous on their end as it is not reasonably likely that it is attributable to an individual. When evaluating the potential for re-identification, it is for instance essential to consider the legal and contractual agreements in place. These agreements can play a crucial role in preventing the attribution of data to a natural person which must be considered as part of the assessment of whether any "reasonable means" for identification are available.

7. Furthermore, the Guidelines state in §43 that in cases where the level of security is only appropriate for pseudonymised data, "all means available" to unauthorised parties that might access the pseudonymised data need to be considered, and not just those that are reasonably likely to be used. The statement in §43 therefore conflicts with the one in §22 and the views expressed in the opinion of Advocate General Spielmann.

8. The Guidelines state in §23 that "*if a controller processes personal data and applies pseudonymisation in the process, then the legal basis for the processing of the personal data extends to all processing operations needed to apply the pseudonymising transformation*". This implies that a separate consent process would be required for carrying out the pseudonymisation process in situations where consent serves as the legal basis for processing the personal data. However, obtained consent is sufficient for the purposes of applying the pseudonymising transformation, as it is a technical and organisational measure to protect the personal data.

2.3 Pseudonymisation domain and available means for attribution

9. The Guidelines suggest in §37 that "*the pseudonymising controller when defining the pseudonymisation domain may choose to include persons who are not legitimate recipients of the pseudonymised data but may attempt to gain access to it anyway*". Video Games Europe cautions that this recommendation would render the use of the concept of the pseudonymisation domain practically impossible, in particular if it is intended to be part of a proper risk analysis subject to the requirements of the GDPR. Data controllers will not be able to anticipate which persons may attempt to gain access to the data illegitimately and should not be put in a position that requires them to incriminate persons in this manner. The challenge for the data controllers is even more significant as the EDPB emphasises that it is crucial to ensure that pseudonymised data

is not shared with anyone outside the domain, i.e. a specific, predefined group. It is unrealistic to expect controllers to guarantee that this data will remain undisclosed beyond that group as they may not be able to clearly identify all individuals beforehand. The Guidelines should be modified to avoid putting controllers in an untenable position. They should only apply within the context of processing activities that are both lawful and fair.

2.4 Meeting data protection requirements using pseudonymisation

10. §47 of the Guidelines sets out a list of conditions which would ensure that data minimisation, confidentiality, and purpose limitation are effectively implemented when pseudonymisation is applied in internal processing. While all three conditions appear to convey the same notion, two of them state that the persons handling the pseudonymised data should not be *able* to reconstitute the data or single out the data subject. We would recommend the rephrasing of these two conditions as it is unclear whether the mere technical ability to reconstitute the data is intended in this context or whether they refer to the ability to have the necessary access and authorisation to perform these operations.

11. We would also recommend the rephrasing of §59 of the Guidelines which states that "*No one in the pseudonymisation domain, who accesses the pseudonymised data without authorisation, should be able to easily use the data to the disadvantage of the data subject, unless they also manage to (illegitimately) access the relevant additional information needed for attribution".* The sentence is not easily readable and gives the impression that exploitation of the pseudonymised data would be permissible.

12. The Guidelines state in §63 that pseudonymisation may constitute a so-called "supplementary measure" to ensure compliance with Arts. 44 and 46(1) GDPR. They clarify that "*pseudonymisation may constitute an effective measure to protect personal data transferred to a third country from disproportionate government access by public authorities of that country if the conditions enumerated in paragraph 85 of Annex 2 to the EDPB Recommendations 01/2020 are fulfilled"*. §64 further explains in bullet 2 that one of the conditions entails that "*additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA".* This seems to refer to the scenario of a transfer based on adequacy, rather than one subject to appropriate safeguards pursuant to Art. 46(1) GDPR. Furthermore, the Guidelines then state that "*this implies that the public authorities, who would be able to have access to the pseudonymised data based on foreign law or practice, need to be framed within the pseudonymisation domain*". This would go beyond what can be expected from supplementary measures under the GDPR.

13. The Guidelines recommend in §65 to start with "*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." The last part of this sentence requires data controllers to consider practices that lie outside the legal framework of the recipient country. It is impossible for any private company to determine if and how public authorities of a third country may be expected to illegitimately access a certain type of information. Video Games Europe, therefore, recommends the deletion of this part of the sentence.

2.6 Implications for the rights of the data subjects

14. The Guidelines explain in §77 that "*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, "*the rights of the data subjects enumerated in Art. 11(2) or 12(2) GDPR, respectively, shall not apply in this case*." These rights do not apply since the controller is not processing personal data. Where the controller does not have "the means reasonably likely to be used" for identification (see §22) and is demonstrably unable to identify the data subject, this pseudonymised data cannot be considered personal data for that controller. Video Games Europe calls on the EDPB to clearly state this in the Guidelines.

15. Where the controller is able to demonstrate that it is not in a position to identify the data subject, Art. 11.2 GDPR requires it to inform the data subject accordingly but only if that would be possible. The Guidelines then further specify in §79 that the information provided in this context needs to include how data subjects can obtain the pseudonyms relating to them, in order to give full effect to the rights of data subjects, and that the "*controller may need to provide the identity and the contact details of the source of the pseudonymised data or of the pseudonymising controller*". Video Games Europe requests clarification whether this information should be given to data subjects reactively or proactively, such as in privacy notices. Furthermore, we caution that the requirement to provide the identity and the contact details of the source of the pseudonymised data may increase the risk of unauthorised or unlawful processing and accidental loss of the pseudonymised data. This requirement conflicts with the requirement under the Art. 5.1(f) to ensure security and protection of the processing of personal data by using appropriate technical and organisational measures and could result in risks to data subjects. Providing such information to data subjects could therefore negatively impact their fundamental rights and freedoms.

About VIDEO GAMES EUROPE

16. Since 1998, Video Games Europe has ensured that the voice of a responsible games ecosystem is heard and understood. Its mission is to support and celebrate the sector's creative and economic potential and to ensure that players around the world enjoy the benefits of great video game playing experiences. Video Games Europe represents 19 European and international video game companies and 13 national trade associations across the continent. Europe's video games sector is worth €24.5bn, and 53% of Europeans are video game players. We publish a yearly Key Facts report with the latest data on Europe's video games sector.

VIDEO GAMES EUROPE Secretariat, February 2025