

Public Consultation on the EDPB's Guidelines 02/2026 on Anonymisation

Response from VIDEO GAMES EUROPE

Transparency Register Identification Number: 20586492362-11

1. Video Games Europe welcomes the opportunity to provide comments on the anonymisation 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 should focus more on offering practical guidance on how to apply the concept of anonymisation in a realistic environment. Such an approach should consider the facts that increase or reduce realistic identifiability and explain how those facts are weighed in context. The Guidelines should adequately implement the CJEU caselaw[1] and provide a non-exhaustive framework for applying the likelihood standards in both directions, including the availability and quality of auxiliary data, cost, time, expertise, computing resources, access conditions, safeguards, and the practical probability that identification would succeed.

3. 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:

    - The Guidelines should acknowledge the possibility that a processor may process only anonymised data in certain circumstances, taking into account the controller's instructions, the scope and volume of the shared data, and all applicable contractual, technical and organisational measures.
    - The Guidelines should align the onward transfer test in §21 with the 'insignificant in reality' standard in §22, rather than a 'cannot be ruled out' threshold.
    - The Guidelines must recognise the difference between the mere existence of the possibility of unauthorised or malicious access against having clear indications that such a situation is reasonably likely to occur.

[1] *Breyer v. Bundesrepublik Deutschland* (C-582/14, EU:C:2016:779).

- The Guidelines should recognise the crucial role that contractual agreements can play in preventing re-identification as part of the assessment of whether any "reasonable means" are available.
- The Guidelines should provide practical guidance on handling outlier records in large datasets, so that a small number of records does not bring an entire dataset within the GDPR.
- The Guidelines should recommend that documentation requirements remain proportionate to the risk, in line with the accountability principle in Articles 5(2) and 24 GDPR, and that periodic reassessment of the anonymisation processing be triggered by material changes, such as security incidents.
- The Guidelines should state clearly that the contextual approach represents the legal test and that the simplified approach remains an alternative option.
- The Guidelines should provide an overview of the various techniques that are used by organisations to alter or combine data to prevent re-identification and explain how the three criteria should be evaluated against these techniques.
- The Guidelines should explain at what point the information that can be revealed from inferring record-level data by analysing and/or combining one or more aggregate datasets is sufficient to conclude that re-identification of an individual is reasonably likely to occur.
- The Guidelines should focus more on AI-related use cases such as AI model training and synthetic data generation.

Detailed analysis

2.2 Identifying the applicable perspective(s)

4. The Guidelines explain in §15 that "*if an entity processes information on behalf of another, whether the given data is personal for that entity should be assessed by reference to the controlling entity's perspective. In practice, this means that if an entity processes information on behalf of a controller (i.e. someone for whom the information is personal data, and who decides the purposes and means of the processing), that information should also be considered personal data for the processing entity.*" Such a "teleological" approach is inconsistent with the principle established in the EU Court of Justice's ruling on the **EDPS vs. SRB case** (Case C-413/23 P) that "*pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject*".

5. This ruling further confirms that contractual and technical means can be put in place as to prevent the data in question from being attributed to the data subject, and that account should be taken of all the means reasonably likely to be used by the controller or '*by another person*'.[2] The Guidelines should therefore acknowledge the possibility that a processor may process only anonymised data in certain circumstances, taking into

[2] See §75 and §79 of CJEU Case C-413/23 P

account the controller's directions, the scope and volume of the shared data, and all applicable contractual, technical and organisational measures.

6. Similarly, example 3 in §15 depicts a situation in which a third-party analytical agency must treat data as personal because the retailer (controller) must do this, but it does not explain why the retailer's ability to identify people should automatically be treated as the agency's ability too. The example should clearly explain what data is shared, what other information the agency can access, what it is allowed to do, and what safeguards are in place.

2.4 Whether the natural person is "identified or identifiable"

7. The Guidelines state in §21 that data should be considered personal for a transfer, and any subsequent processing by the recipient if it is reasonably likely that an entity can transfer the data to a third party and "*it cannot be ruled out"* that the recipient has the means to identify the individual. The data would then also become personal for the transferring entity. This sets a much lower threshold than the standard in §22, under which the likelihood of identification need not be zero but should be insignificant in reality. A 'cannot be ruled out' test comes close to requiring zero risk, which the CJEU has rejected. VGE recommends that §21 be aligned with §22, so that data becomes personal only where identification by the recipient is reasonably likely, assessed on the basis of objective factors.

8. The Guidelines depict in §28 (example 7) a situation in which a controller wants to share anonymised data with its business partner but realises that the data subjects could be re-identified through a certain re-identification technique if the business partner would hire a third party to do so. The assertion that the controller's business partner "could easily hire" a third party to engage in re-identification does not constitute a reasonable threshold to assess the risk of re-identification. The example seems to focus on the theoretical possibility of re-identification rather than the likelihood of it occurring in practice. In reality, a business partner may have little or no incentive to engage a third party for this purpose, particularly given the associated costs, time and resources required. This scenario also improperly ignores critical safeguards, including contractual restrictions, that would prohibit and deter such actions. Video Games Europe recommends drawing a clearer distinction between what is technically possible and what is reasonably likely to occur in practice.

9. The Guidelines provide in §30 a list of entities that can be relevant for the assessment of whether a person is identifiable. This list comprises anybody directly or indirectly receiving the data, including unauthorised and malicious actors. While footnote 25 states that "*not all of these perspectives would need to be considered systematically in each case but this depends on the circumstances of each specific case and the entities directly or indirectly receiving the data*", it should be made more explicitly clear that these entities are relevant only where the facts show a realistic likelihood that those

actors will gain access to the information and can successfully re-identify an individual. The Guidelines must recognise the difference between the mere existence of such actors or the abstract possibility of unauthorised access and clear indications that re-identification is reasonably likely. A proper risk analysis should consider actual evidence such as access pathways, the actor's capabilities, the strength of security controls, prior incidents, monitoring and enforcement, real incentives, and the practical likelihood that an attempted identification would succeed. In relation to the latter, Video Games Europe recommends that the EDPB provides further clarity on how likelihood should be established from a practical and operational point of view.

10. Furthermore, §31 provides for the example that identification may occur due to an accident or negligence beyond an entity's willingness or motivation. We agree that subjective intentions may be difficult to demonstrate. However, objectively evidenced incentives and disincentives should remain relevant and §31 itself recognises this by requiring the value of re-identified data, and the risks of re-identification for itself, to be considered. The Guidelines should make clear that such objective factors are part of the assessment. They should also state that an accident or negligent act matters only where it is reasonably foreseeable in the circumstances, rather than treating any conceivable mistake as a means reasonably likely to be used.

11. We accept that a contractual prohibition is not a prohibition by law (§34). However, the categorical statement that contractual measures "*should only be used to complement technical measures"* sits uneasily with the requirement to assess all objective factors in §29. We suggest that contractual measures which are reliable, verifiable and enforceable, for example through audit rights, monitoring, penalties and termination rights, should be given weight analogous to the presumption applied to legal prohibitions in §32 & 33, rebuttable by the same kind of evidence. The Guidelines should also clarify that §90's statement that such measures are "*not by themselves sufficient*" does not mean they carry little weight in the overall assessment.

2.5 Additional considerations

12. §36 provides that a dataset should only be considered anonymous if anonymisation is effective for every individual it contains, and that otherwise the entire dataset should be treated as personal unless its parts are treated separately. For very large datasets, a small number of outlier records could therefore bring the whole dataset within the GDPR, particularly when read with §87. We welcome the recognition that separate treatment is possible and suggest that the Guidelines explain what it requires in practice. In particular, it would help to confirm that outlier records can be suppressed or held separately as personal data, so that the remainder of the dataset, once re-tested against the three criteria, can be considered anonymous.

13. The Guidelines state in §40 that controllers should not use descriptions like 'anonymous', 'de-identified' or 'de-personalised' if individuals are actually still

identifiable. We would like to point out that the latter two terms are widely used to indicate that de-identifying measures have been applied to data, but that the resulting dataset may not meet the standard for anonymity. The Guidelines should acknowledge that many organisations already use these terms to describe different levels of identifiability.

14. The Guidelines call in §41 and §42 for adequate documentation, including demonstration of the compliance and the effectiveness of anonymisation, and periodic reassessment of the anonymisation processing. They do not provide details about the frequency of these requirements which could create legal uncertainty. The Guidelines should recommend that documentation requirements remain proportionate to the risk, in line with the accountability principle in Articles 5(2) and 24 GDPR, and that periodic reassessment of the anonymisation processing be triggered by material changes, such as security incidents. Furthermore, it would be useful to provide clarity on how the effectiveness of anonymisation should be demonstrated from an operational standpoint.

3.2 Approaches to the assessment

15. The Guidelines introduce in §48 the simplified approach as a way to voluntary to shift the risk from false positives to false negatives whereby the controller treats all data as personal. While it is stated that the simplified approach is not an alternative legal standard, there is a risk that it will replace the contextualised approach, systematically overclassifying data as personal even where it would be anonymous. In particular, the complexity and potentially resource-intensive nature of the contextual approach may lead organisations, especially those with limited resources or expertise, to default to the simplified approach. The Guidelines should state clearly that the contextual approach represents the legal test and that the simplified approach remains an alternative option. More practical guidance from the EDPB is needed to ensure that the contextual approach remains a viable option.

16. Example 9 in §49 appears to compare how the simplified and contextual approaches can be applied to the anonymisation of a dataset containing a combination of demographic and medical information. It does not, however, draw any conclusion from the contextual assessment, nor does it show how the two approaches differ or whether they would produce different outcomes. Video Games Europe recommends elaborating on these points which would make the example more useful.

3.4 The three criteria

17. The Guidelines introduce a pathway to technical analysis of anonymisation based on the three criteria (No Record Isolation, No Linkage and No Inference) that were also identified in the previous Guidelines on Anonymisation Techniques by the Article 29 Data Protection Working Party (Opinion 05/2014). They however do not provide an

overview of the various techniques that are used by organisations to alter or combine data to prevent re-identification, nor do they explain how the three criteria should be evaluated against these techniques. It would be helpful to have this clarified in the Guidelines.

18. The Guidelines state in §77 that it may be possible to infer record-level data by analysing and/or combining multiple aggregate datasets, and that "*this is particularly true for advanced de-aggregation techniques, including attacks which can extract data from supposedly anonymous AI models*". At the same time, they claim that a single dataset which contains a sufficiently large quantity of data may also allow for the inference of information relating to a single individual, without the need for other sources. The Guidelines however do not explain at what point the information that can be revealed is sufficient to conclude that identification of an individual is reasonably likely in practice. Similarly, example 18 in §79 does not explain how it should be assessed whether membership inference is technically possible and reasonably likely.

3.5 Applying the criteria

19. §83 states that "*The three criteria set out above should be used to evaluate the effectiveness of (re-) identification techniques that can be deployed against the given data*." The requirement could be interpreted as having to use the three criteria to perform reverse engineering assessments of such technologies to then demonstrate and evidence full anonymisation, in avoidance of re-identification. Such an assessment would be very resource-intensive, in particular for smaller companies. The Guidelines should provide practical clarity of what level of assessment is required.

20. Furthermore, some parts of section 3.5 risk making the assessment stricter than the law requires. §87 treats anonymisation as failed if re-identification works against even one individual (see our comment on §36 above). §88 calls for "adequate safety margins" but gives not guidance on what is adequate, which may lead organisations to treat anonymous data as personal just to be safe. §92 assumes that time and cost are not generally a barrier to re-identification, but the CJEU has recognised that disproportionate effort can make identification unlikely. This should be assessed on the facts of each case, especially as §92 itself accepts that obtaining the additional information needed for re-identification can be difficult.

21. The Guidelines recognise that AI may increase the re-identification risk, both by reducing the time and cost of gathering information (§92 & §93) and through inferences drawn from AI models and synthetic data (§82). The Guidelines however do not explain how these risks should be assessed in practice. Video Games Europe would welcome more specific guidance in relation to AI-related use cases such as AI model training and synthetic data generation, in particular on how such models and datasets should be tested against the three criteria, what level of resistance to extraction or inference attacks is sufficient, and how this guidance related to Opinion 28/2024.

About VIDEO GAMES EUROPE

22. Since 1998, Video Games Europe has ensured that the voice of a responsible video 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. Europe's video games sector is worth €29.7 billion and accounts for 123,000 jobs. 51% 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, October 2026