CONTRIBUTION TO CONSULTATION

EDPB GUIDELINES 02/2026 ON ANONYMISATION

MFE-MEDIAFOREUROPE brings together leading media brands across broadcasting, VOD and audiovisual production, with operations in Italy, Spain, Germany, Austria, Portugal and Switzerland. Reaching 220 million viewers and employing approximately 13,000 people, the Group is committed to cultural diversity, media pluralism, accountability and consumer protection. MFE reinvests most of its advertising revenues in European content, including films, series, entertainment and professional news.

A) Review of the relevant data protection issues and proposed amendments

The Guidelines under consideration adopt a risk-based approach to identifiability, whereby the same dataset may constitute personal data for one entity and anonymous data for another, depending on the means "reasonably likely" to be used for re-identification. While, on the one hand, this approach reflects the case law of the Court of Justice, on the other hand it makes the classification of the data dependent upon a predictive assessment lacking any common threshold or methodology, thereby placing on the parties involved (in particular, the controller) a significant assessment and documentation burden. In this respect, the Guidelines do not appear to deliver any tangible benefit in terms of "simplification"; rather, they add a further layer of detail and complexity to an already complex landscape. The suggestions set out below should be read in this light.

1. Indeterminacy of the predictive criterion and legal certainty

This issue arises, *inter alia*, in paras. 27-29 and in Examples 7-8: the Guidelines link anonymity to a "*insignificant likelihood in reality*" of re-identification, without specifying either a threshold or a common calculation methodology, or the manner in which such likelihood is to be measured and monitored. As a result, each operator — including large platforms — could settle on different values, to the detriment of legal certainty and equal treatment; a reference scale appears indispensable to ensure that the assessment is not left to the discretion of each individual operator.

2. Allocation of the burden and liability

Identifiability is assessed from the perspective of the individual entity and by reference to the means "*reasonably likely to be used*" by it, including those obtainable by leveraging the capabilities of third parties (para. 29). It remains unclear who bears the burden of assessing the means available to the recipient and according to which criteria: the entity carrying out the anonymisation or the transfer would be compelled to base its assessment on elements falling within another party's sphere, which it cannot

verify, with the risk of a de facto strict liability, at odds with the accountability principle. This indeterminacy is compounded where one considers, as the Guidelines do, that the means "reasonably likely" to be used also include the possibility of instructing a third party to carry out the re-identification (Example 7); since almost anyone could, in the abstract, turn to a third party, the criterion risks rendering re-identification always "reasonably likely" and turning the proof of anonymity into a *probatio diabolica*.

3. The scope of the relevant scenarios and actors: actual recipient or malicious third party

A particularly important observation concerns the range of actors in relation to whom identifiability is to be assessed. In certain passages (see Example 8, concerning a *media company* with outdated security measures), the analysis does not stop at the actual recipient of the data, but requires consideration of the possibility that an unspecified unauthorised third party — a malicious actor breaching the systems — may access and re-identify the data. Identifiability thus ends up depending not on the means available to the actual recipient, but on the robustness of the security measures against hypothetical attacks, improperly conflating anonymisation with security. The overall effect is a worst-case test, further reducing predictability.

4. The dynamic nature of anonymity and the burden of proof

The Guidelines conceive of anonymity not as an intrinsic and stable property of the data, but as a relative and reversible status: the likelihood of re-identification tends to increase over time, owing to technological progress and the growing availability of additional information, and may eventually exceed the relevance threshold, with the consequent re-classification of the data as personal data. In the writer's view, this aspect constitutes one of the key issues of the consultation: it places on the controller a peculiar burden of proof — that of proving a negative fact, namely the absence of any reasonable possibility of re-identification — which is, moreover, ongoing, without the Guidelines specifying the conditions for, and the frequency of, the re-assessment, or the effects of a supervening re-classification on processing operations carried out in the meantime on the assumption of anonymity. It would be advisable for the EDPB to define such conditions and to mitigate the burden, allowing for presumptions of adequacy where state-of-the-art techniques are employed. It should also be borne in mind that the identifiability assessment relates to the time at which it is carried out and to the circumstances existing at that time, which are liable to change over time. Since continuous repetition of the assessment cannot reasonably be required, it should be deemed valid as at the time it was carried out, save where new and relevant elements subsequently arise. Consistently with the principle of proximity of evidence, it should moreover fall to the recipient of the data — the only party aware of the means actually available to it — to report any supervening re-identifiability, without the "transferring" controller being subject to an open-ended monitoring obligation.

5. Relationship with pseudonymisation

Example 2 and the entire related framework rely on the EDPS v SRB judgment (Court of Justice, Case C-413/23 P, 4 September 2025), which, however, concerns *pseudonymised* data, not anonymised data. Transposing the logic of relativity — developed for data that remain personal and re-identifiable by the controller — to the notion of anonymisation, which is irreversible by definition, risks conflating the two concepts and, in particular, classifying as anonymous pseudonymised data protected by strong encryption.

6. Permitted techniques, cumulative application of the two approaches and internal consistency

The technical analysis sets out two approaches (contextual and simplified: section "Approaches to the assessment"; Example 9) and three criteria (No Record Isolation, No Linkage and No Inference), but does not make it unequivocally clear whether the two approaches are cumulative or alternative. Their sequential application appears to emerge as best practice, yet the Guidelines do not lay down a general rule on the point. Moreover, the relationship between the technical analysis and the legal analysis, as well as the placement of the assessment of the effectiveness of re-identification techniques, which appear to partially overlap, remain unclear: the interplay between criteria, techniques and the sequence of implementation should be clarified.

7. The position of the processor and the presumption of re-identifiability

The approach that the Guidelines apply to entities processing the data independently (see Example 4, concerning the research institute) is not, however, extended to the processor. Paragraph 15 and Example 3 in fact provide that, where an entity processes data on behalf of the controller, identifiability is not assessed from the perspective of that recipient: the processor is not regarded as an autonomous recipient for the purposes of the re-identification assessment, and the data are classified as personal data for that entity as well, solely because they are personal data for the controller. In so doing, however, the processor's ability to re-identify the data subject is taken for granted — an ability which, in practice, may be lacking where the processor does not have the necessary means and additional information. The *per relationem* rule, while consistent with the aim of preventing circumvention of the GDPR through the outsourcing of processing, thus amounts to a presumption that disregards any verification of the means actually available to the processor, at odds with the very relative approach — and with the definition of personal data put forward in the so-called Digital Omnibus, according to which: "*Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity*...")[2]; the generic reference to an "entity" should therefore, in the abstract, also encompass the processor — an approach which the Guidelines state they adopt. It would be advisable for the EDPB to clarify the conditions for, and the

limits of, such presumption, acknowledging that, where the processor genuinely lacks the means of re-identification, identifiability should also be assessed from its perspective. It should be added that such verification should not, however, translate into an additional burden for the controller that "entrusts" its personal data to the processor; rather, also by virtue of the well-established so-called principle of "proximity of evidence", it would, where appropriate, be for the processor itself to declare and demonstrate that it is unable to identify the information entrusted to it, in order for such information to be regarded as anonymous.

8. Transparency and anonymisation as a form of processing

The very act of anonymising constitutes processing of personal data, which requires a legal basis and compliance with the principles; the Guidelines acknowledge this, but in terms that raise more than one doubt. On the one hand, they characterise anonymisation as a "purpose" of the processing and impose on the controller transparency obligations towards data subjects (Articles 5(1)(a) and 12-15 GDPR; see para. 41) regarding the fact that the data will be processed in order to produce anonymous data; on the other hand, the outcome of such processing falls outside the scope of the GDPR. It should therefore be clarified whether, and in what sense, anonymisation constitutes an autonomous "purpose", and how the information obligation can be reconciled with the fact that the end product is no longer personal data and therefore, in and of itself, falls outside the scope of the GDPR.

9. Documentation burden and proportionality

The Guidelines require detailed documentation of the anonymisation process and of the related tests, to be retained even after the process has been completed. When added to the documentation already required for each processing operation, such documentation burden — in itself consistent with the accountability principle — may become, in the absence of clear assessment criteria and in the event of a particularly strict application of the Guidelines, disproportionate overall to the simplification objective declared at EU level. From an operational standpoint, a documentation and assessment burden so configured is also liable to affect the timing of contractual negotiations, lengthening them, with non-negligible practical implications for operators. It is also to this accumulation of obligations — and not to the documentation alone — that the "significant burden" referred to in the introduction relates.

Proposed amendments

While leaving it to the EDPB to carry out any broader assessment of all the issues raised above, a number of targeted proposals for amendments to the text of the Guidelines under consideration are set out below.

- It would be advisable to provide a common methodology and an anonymisation assessment template, with objective factors and a clear reference threshold for the likelihood of re-identification,

along the lines of the template and common methodology envisaged, for example, for the data protection impact assessment under Article 35 GDPR.

- It is suggested that the scope of the relevant actors and scenarios be limited to the actual recipient and to the means actually available to it, so that anonymity does not depend on hypothetical attacks by malicious third parties or solely on the robustness of the security measures.
- It would be advisable to clarify the conditions for, and the frequency of, the re-assessment of anonymity over time in light of technological progress — including developments in computing power and their impact on the robustness of cryptographic techniques — as well as the effects of a supervening re-classification. It should also be specified that such assessment relates to the time at which it is carried out, since continuous repetition cannot reasonably be required, and that the burden of reporting any supervening re-identifiability should fall on the recipient of the data, pursuant to the principle of "proximity of evidence".
- Consistency with EDPB-EDPS Joint Opinion 2/2026 should be ensured, so that the approach set out in the Guidelines does not, by way of interpretation, narrow the current notion of personal data and the scope of application of the GDPR.
- It is suggested that the conditions for, and the limits of, the rule whereby the processor is not assessed as an autonomous recipient for re-identification purposes (para. 15; Example 3) be clarified, avoiding any presumption of its ability to re-identify the data subject and acknowledging that, where it actually lacks the necessary means, identifiability should also be assessed from its perspective.
- It would be advisable to specify whether the two approaches (contextual and simplified) are cumulative or alternative, as well as to clarify the relationship between the legal analysis and the technical analysis and eliminate overlaps between sections, indicating the techniques deemed appropriate.

MFE – MEDIAFOREUROPE N.V., 29 October 2026

Transparency Register's ID: 91471238809-21