PIERSTONE

To the attention of:

Ms Anu Talus
Chair
European Data Protection Board (EDPB)

And,

Ms Isabelle Vereecken, Head of the Secretariat, EDPB

Brussels, 27 October 2026

Public consultation on Guidelines 02/2026 on anonymisation: comments and proposed amendments

Dear Ms. Talus,

Pierstone BV, an international law firm based in Brussels specialising in data, artificial intelligence and digital law, welcomes the EDPB's initiative to open its Guidelines 02/2026 on anonymisation, adopted on 7 July 2026 (hereinafter the 'Guidelines'), for public consultation. This long-awaited update to Opinion 05/2014 of the Article 29 Working Party represents an important opportunity to clarify a central concept of the GDPR, the scope of which directly determines the responsible use of data across all economic sectors.

We particularly welcome the recognition, in paragraphs 7 to 12 of the Guidelines, of the relative ('contextual') nature of the concept of personal data, as established by the Court of Justice of the European Union (CJEU) in the EDPS v SRB judgment (C-413/23 P). This clarification was necessary.

On closer examination, however, several aspects of the Guidelines appear to us to undermine these advances in practice and create substantial legal uncertainty for economic operators. We wish to draw the EDPB's attention to the following points, and then set out specific proposals for amendments.

1. The status of the data processor. Paragraph 15 of the Guidelines aligns the classification of the data processor with that of the data controller, through a 'teleological application' of the GDPR. Presented as deriving from the EDPS v SRB judgment (via Example 2, paragraph 14), this rule in fact goes beyond what the Court ruled: the CJEU's reasoning in that judgment related strictly to the scope of the obligation to provide information (Article 15, paragraph 1(d) of Regulation 2018/1725, a provision analogous to Articles 13(1)(e) and 14(1)(e) of the GDPR) at the time of collection, not on a general rule of classification applicable to any purpose.

The Guidelines themselves, in paragraphs 7–12, set out a general contextual approach: identifiability is assessed on a per-entity basis, according to the means reasonably likely to be used by that entity. Paragraph 15 introduces an unexplained exception to this general principle solely for the category of data processors, without justifying why this category of entity would be exempt from the methodology that the EDPB applies to all others. A comparison of Examples 3 and 4 is revealing: the data received by the agency (Example 3) and by the research institute (Example 4) may be exactly the same, and the means available to these two entities equally comparable; it is solely their legal status (acting 'on behalf of' or independently) that changes the outcome. However, Recital 26 of the GDPR requires that

identifiability be assessed in the light of 'all objective factors', and not on the basis of the entity's contractual status.

Moreover, this exception is not necessary to avoid the risk of circumvention that the EDPB seeks to prevent (a controller outsourcing to evade the GDPR), as this risk is already covered by the 'chain of means' test (§20–21, §28) which the Guidelines apply to any entity. Thus, if the processor has de facto access to the means of re-identification (because it belongs to the same group, because it can request them from the controller, because the data is returned to it in an enriched form, etc.), it remains classified as an entity processing personal data under this contextual test, without the need for an additional categorical rule in §15. Conversely, the rule in §15 produces results that are difficult to justify: a service provider that receives only pseudonymised identifiers, without a key or any reasonable means of accessing them, would be subject to all the obligations set out in Articles 28 to 33 and 37 of the GDPR, and the transfer to that service provider outside the Union would have to be regulated under Chapter V (note 12), even though the data are, for that service provider, anonymous within the meaning of paragraphs 7–12. Such an outcome does not provide any greater protection for data subjects; it diverts compliance resources towards processing operations which, for the entity concerned, present no risk of identification. Such compliance efforts may divert attention and resources away from innovation.

2. 'Means reasonably likely to be used'. The proposed test (§26 et seq., §49) applies a standard of absolute impossibility, whereas the CJEU (SRB, §82–83) applies that of means that are 'impossible in practice' to mobilise in order to achieve a probability of re-identification that is, in reality, 'insignificant'.

The Court has, however, been clear*: 'In addition, the Court has previously held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour (see, to that effect, judgment of 7 March 2024, OC v Commission, C-479/22 P, EU:C:2024:215, paragraph 51 and the case-law cited). That case-law bears out the interpretation that the existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725.'* (EDPS/SRB, paragraph 82).

The test as formulated by the EDPB requires proof of a universal negation, including with regard to hypothetical or unlawful actors (hackers, dishonest employees, intelligence services, §30 and §32), concerning any future technological developments, **which results in a standard of proof that is, in practice, impossible to meet with certainty**. The role of intent, whilst relevant to assessing whether identification is reasonably foreseeable, is furthermore explicitly ruled out in §31. Zero risk is unrealistic.

The mere fact that a situation of re-identification is 'possible' does not mean that it is 'reasonably likely'. An interpretation that equates 'possible' with 'reasonably likely' would render the concept of anonymous data entirely meaningless, whereas the Court points out that the concept of 'personal data' is not unlimited and requires, inter alia, that the data subject be identified or identifiable (EDPS/SRB, paragraph 88).

Furthermore, this approach contradicts the opinion of the EDPB provided to the European Commission in its letter of 5 May 2026, in which the EDPB takes a more flexible stance regarding the outcome of anonymisation and the 'overall' risk of re-identification, which must, in practice, be insignificant (see below).

Finally, a concept of personal data without any practicable limits runs counter to the Union's objective of creating a single data market and supporting European innovation and competitiveness. In this regard, we note that the 'Digital Omnibus' proposal for a regulation presented by the Commission on 19 November 2025 aims to enshrine in Article 4(1) of the GDPR the approach established by the EDPS v SRB judgment. Whatever the outcome of this proposal, the Guidelines would benefit from being drafted in a way that remains consistent with this approach, so as to avoid organisations having to revise their assessments in the near future.

3. Contractual measures. Paragraph 34 treats any contractual limitation as insufficient in principle, on the grounds, in particular, that the parties might revise or fail to honour their commitments:

'A prohibition set out in a contract (even if it is legally binding upon its parties) should not be treated as a prohibition by law. […] bearing in mind that contractual measures can typically be subject to revision, or may even be disregarded entirely by the parties.' (Paragraph 34 of the Guidelines)

Contracts have always served as a tool for risk management. In the context of anonymisation, contractual measures should be recognised by the EDPB as safeguards in their own right, capable of effectively complementing technical measures to prevent the risk of re-identification. What is lacking are criteria for determining when and to what extent a contractual safeguard reduces the probability of identification. A contract containing an express prohibition on re-identification and linking, audit rights, sanctions (termination, penalties, liability), obligations extended to sub-recipients and an appropriate duration is 'reliable, verifiable and enforceable' within the meaning of §34 (Joint DMA/GDPR Guidelines, §181). Foreign regulatory frameworks (for example, the 2025 Ontario model) also explicitly incorporate contractual controls into the assessment of the probability of an attack.

Furthermore, in its aforementioned letter of 5 May 2026, the EDPB confirmed that contractual measures, in addition to technical measures, may be sufficient to reduce the residual risk of re-identification. We support this approach as it takes into account the objective factors referred to in Recital 26 of the GDPR. Admittedly, the EDPB makes the consideration of contractual measures conditional upon them deriving from a binding implementing act; however, what makes these measures effective is not necessarily the source of the obligation, but rather its durable, verifiable and enforceable nature (see footnote 12 of the annex to the letter, according to which the effects of the implementing act 'should be both durable and verifiable', and §34 of the Guidelines). These characteristics may be achieved by contractual means. The EDPS v SRB judgment (C-413/23 P) does not rule on contractual measures either and cannot be relied upon in support of this specific position.

'Regarding anonymisation of end users' personal data in the specific context of Article 6(11) DMA, the EDPB recalls that technical measures for the alteration of the data can be complemented by organisational, administrative and contractual measures, when they derive from legally binding requirements imposed on the gatekeepers through an implementing act, to mitigate the residual risk of re-identification. The technical measures must provide a sufficiently robust level of protection of personal data which, in the context of Article 6(11) DMA, can be complemented by contractual measures imposed via an implementing act. While, in some cases, a residual risk of re-identification

remains, the result of an anonymisation process should be that such overall risk of re-identification is, in practice, insignificant.' (point 7 of the annex to the EDPB's letter to the European Commission of 5 May 2026, specification procedure concerning Alphabet, Article 6(11) of the DMA)

4. Mixed datasets. Paragraph 36 provides that an entire dataset must be treated as personal data as soon as any part of it is personal data and the parts are not 'treated separately'. This rule is based, in footnote 31, on the Meta v Bundeskartellamt judgment (C-252/21, paragraph 89), which, however, concerned a separate issue: the combined processing of sensitive and non-sensitive data within the meaning of Article 9 of the GDPR within a dataset already classified as personal data, and not the threshold for classifying data as personal data per se. Furthermore, the concept of parts that are 'treated separately' is not defined. We propose that §36 specify that, where records for which anonymisation is not effective can be identified and technically isolated (for example, by flagging, partitioning or deletion), only those records fall within the scope of the GDPR, whilst the remainder of the dataset retains its anonymous nature.

5. The 'No Record Isolation' criterion and the concept of identification. The Guidelines (§54 et seq., Example 5) appear to elevate 'singling out' – mentioned in Recital 26 of the GDPR as a mere example of a means of identification – to the status of a self-sufficient test of identifiability. This goes beyond the definition adopted by the Article 29 Working Party in 2014 (singling out as a necessary but not sufficient condition) and appears to conflict with the definition of **identification** given by the Guidelines themselves (§19), **which requires the possibility of treating the individual differently, not merely distinguishing them within a given context.**

The cumulative effect of these factors **significantly complicates** the assessment process and places a **disproportionate burden of proof** on organisations, **without providing the legal certainty** that guidelines are intended to offer. We fear that, in practice, this will discourage the use of data that has nevertheless been validly anonymised, to the detriment of the data subjects themselves, who have a vested interest in organisations prioritising anonymisation over the processing of identifiable data.

Practical solutions: proposed amendments

In order to strengthen legal certainty whilst preserving the protection objective pursued by the EDPB, we propose the following amendments:

- **§15 –** to remove the categorical rule in §15 which automatically attributes to the processor the classification applied to the data controller, and instead to assess the processor's status using the same contextual methodology as that applied by the Guidelines to any other entity (§7–12, §20–21, §28), that is to say, on the basis of the data processor's own means reasonably likely to be used, including the 'chain of means' test already provided for in the Guidelines, which is sufficient to address the risk of circumvention without requiring an unjustified categorical exception. In the alternative, to limit §15 to cases where the processor has access, either de facto or upon simple request, to the means of re-identifying the controller;
- **§21 –** to replace, in §21(b), the words 'it cannot be ruled out that this receiving entity has the means' with 'it is reasonably likely that this receiving entity has the means', in order to bring the text into line with Recital 26;

- **§26–33 and §49 –** to confirm, in the body of §26 to §33, the standard adopted by the CJEU ('impossible in practice' / 'insignificant in reality') and to exclude unlawful or purely hypothetical means from the test of 'means reasonably likely to be used', as these elements fall within the scope of the security risk analysis within the meaning of Article 32 of the GDPR, unless there is concrete evidence, in the specific case, of a real risk within the meaning of §33; to specify in paragraph 31 that the value of the data and the risks incurred by the entity carrying out the re-identification constitute objective indicators of the likelihood of an identification attempt; and to incorporate footnote 36 into the main text of paragraph 48, expressly stating that the simplified approach cannot form the basis for a supervisory authority's determination that data are personal;
- **§34 –** to redraft §34 so as to set out the criteria that contractual measures must meet in order to be taken into account when assessing the means reasonably likely to be used: (i) an express prohibition on re-identification, linking and attempts at re-identification; (ii) rights of verification and audit; (iii) effective sanctions (termination, penalties, liability); (iv) extension of obligations to sub-recipients; (v) permanence, not subject to unilateral revision; (vi) documentation. Contractual measures meeting these criteria would be deemed 'reliable, verifiable and enforceable' and taken into account, alongside technical measures, to reduce residual risk, in accordance with the position expressed by the EDPB on 5 May 2026[1] ;
- to supplement the qualitative standards ('insignificant risk') with indicative numerical thresholds, by category of sensitivity, constituting a simple presumption of anonymity ('safe harbour') without prejudice to a case-by-case assessment (following the Ontario model, thresholds ranging from 0.05 to 0.09 depending on the degree of privacy infringement, or k-anonymity values of 3 to 5 as set out in the Singapore PDPC guidelines);
- to illustrate, from a methodological perspective, a reproducible risk formula (quantified vulnerability × probability of attack) and a standard list of attack scenarios (deliberate attack, accidental recognition by an acquaintance, data breach), as set out in the Ontario model, as well as a step-by-step methodology accompanied by a reference list of anonymisation techniques and their limitations, modelled on the Singapore guide, with reference to recognised standards (notably ISO/IEC 27559:2022);
- to establish a mechanism of rebuttable presumption, modelled on copyright law (the person exploiting a work is presumed to be its author): provided that the data controller documents that they have followed a recognised methodology in line with the state of the art, the data are presumed to be anonymous and the burden of proof would fall on the authority to demonstrate, in concrete terms, the existence of a means reasonably likely to be used in the specific case;
- **§36 –** to reconsider the reference to the Meta v Bundeskartellamt judgment in §36, to define the concept of parts of a dataset 'treated separately', and to specify that only records for which anonymisation is not effective fall within the scope of the GDPR where they can be technically isolated;
- **§19, §98 and Example 6 –** to clarify that the possibility of treating a person differently constitutes an indicator of identifiability to be assessed alongside the other objective factors

[1] https://www.edpb.europa.eu/system/files/2026-09/edpb_contribution_20260505_consultationec_en.pdf

set out in Recital 26, from the perspective of each entity, and to refine Example 6 in relation to a third party that has no additional information enabling the attribution of an identity;

- to ensure, in coordination with the European Commission and national authorities, a single and consistent standard for anonymisation across the GDPR, the DMA, the Data Act, the EHDS and the European Digital Acquis, including in light of ongoing legislative developments (the 'Digital Omnibus' proposal);

We remain at the EDPB's disposal to discuss each of these points in greater detail, including through detailed drafting proposals, and to contribute, as part of the consultation, to the development of guidelines that both protect data subjects and are operationally feasible for economic operators.

We thank you for your consideration of these comments and proposed amendments.

Yours faithfully,

Pierstone BV

Patrice Vanderbeeken | Partner

Ophélie Snoy | Managing Associate

www.pierstone.be