Response to the EDPB Public Consultation on Guidelines 02/2026 on Anonymisation

Subject

Comments on paragraph 15 and Example 3 — the applicable perspective where data are processed on behalf of another entity

Submitted by: Dr Michele Loi; Avv. Massimo Padovani (Studio Legale Padovani)
Date: 2 October 2026

---

1. Executive summary

We welcome the EDPB's recognition in Guidelines 02/2026 that anonymity is contextual and that the same information may constitute personal data for one entity while being anonymous for another.

We are, however, concerned by the rule introduced in paragraph 15 and illustrated by Example 3, according to which, whenever an entity processes information on behalf of a controller, the personal nature of the information for the processing entity should automatically be assessed from the controller's perspective.

In our view, this rule should be reconsidered.

It does not follow from the judgment of the Court of Justice in **Case C-413/23 P, EDPS v SRB**. On the contrary, the Court established that pseudonymised data need not constitute personal data "in all cases and for every person" and expressly recognised that pseudonymisation may prevent **persons other than the controller** from identifying the data subject, so that the data subject is not identifiable for those persons.

The fact that the recipient acts on behalf of the controller should therefore be treated as an important **contextual factor** in determining what means of identification are reasonably likely to be available to the recipient. It should not operate as an irrebuttable attribution of the controller's identifying capabilities to the recipient.

We propose replacing paragraph 15 and Example 3 with a test based on the recipient's **actual or reasonably available means of identification**, while preserving all GDPR obligations applicable to the controller in relation to its own processing, the anonymisation or pseudonymisation operation, and the disclosure of the data.

---

2. Paragraph 15 goes beyond what was decided in *EDPS v SRB*

Paragraph 15 states, in substance, that where an entity processes information on behalf of another, whether the data are personal for that entity should be assessed by reference to the controlling entity's perspective.

The Guidelines themselves frame this conclusion as following from a **teleological application of the GDPR**, rather than identifying it as a rule established by the Court of Justice.

That distinction is material.

In *EDPS v SRB*, the Court held that the existence of additional identifying information in the possession of another entity does not, by itself, make pseudonymised information personal data "in all cases and for every person". It held instead that the assessment depends on whether the entity concerned has, or may have access to, means reasonably likely to be used to identify the data subject.

Most importantly, paragraph 86 of the judgment expressly states that pseudonymisation may effectively prevent:

> "persons other than the controller"

from identifying the data subject, with the result that, **for them**, the data subject is not or is no longer identifiable.

The Court did not formulate an exception for persons processing on behalf of the controller.

Source:
Court of Justice of the European Union, Case C-413/23 P, *EDPS v SRB*:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0413

EDPB Guidelines 02/2026 on Anonymisation:
https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf

---

3. The controller–recipient relationship was raised before the Court but was not decided

This point is particularly important.

The EDPS specifically argued before the Court that the case differed from *Breyer* because Deloitte was not the controller and was contractually bound to the SRB. On that basis, the EDPS argued that it should not have been required to perform a full assessment of Deloitte's reasonably available means of identification.

The Court did not endorse that proposition.

Instead, after deciding the dispute concerning Article 15 on a separate ground — namely that the controller's transparency obligation had to be assessed at the time of collection and from the

controller's perspective — the Court expressly stated that there was no need to examine the EDPS's arguments summarised in paragraphs 93 and 94.

Accordingly, the effect of a contractual or processor-type relationship on the recipient-specific identifiability test was **left open** by the Court.

This is also consistent with the EDPB and EDPS's own Joint Opinion 2/2026. In February 2026, the EDPB and EDPS expressly acknowledged that the *EDPS v SRB* judgment raises numerous practical and legal questions. As an example, footnote 29 records the question raised by stakeholders whether an entity that cannot reasonably identify the data subject, but processes the data on behalf of a controller, can qualify as a processor.

Paragraph 15 of the draft Guidelines therefore answers categorically, through interpretation, a question that the Court itself did not resolve.

Sources:
CJEU, Case C-413/23 P, *EDPS v SRB*:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0413

EDPB–EDPS Joint Opinion 2/2026 on the Digital Omnibus:
https://www.edpb.europa.eu/system/files/documents/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf

---

4. Processor status should not replace the identifiability test

Article 4(1) GDPR defines personal data by reference to whether a natural person is identified or identifiable.

Article 4(8), in turn, defines a processor as an entity that processes **personal data** on behalf of a controller.

Using processor status to determine whether the information is personal data risks circularity:

> **the data are personal because the entity is a processor, while the entity is a processor because it processes personal data.**

The more appropriate sequence is:

1. determine whether the information constitutes personal data for the relevant entity under Article 4(1), taking account of all means reasonably likely to be used;
2. determine the legal role and obligations applicable to the processing of those data.

A contractual relationship with the controller is clearly relevant to the first inquiry because it may give the recipient access to identifying information. It should not, however, replace that inquiry.

---

5. “On behalf of” is relevant evidence, not a substitute for identifiability

A controller–processor relationship can materially increase the likelihood of identification.

For example, identification may remain reasonably likely where the recipient:

- may request the re-identification key from the controller in the ordinary course of the service;
- receives identifiers through another interface;
- regularly returns outputs that are re-linked to named individuals;
- has contractual, operational or technical access to the controller’s identifying dataset;
- can cause the controller to perform re-identification on its behalf.

In those circumstances, the information may properly remain personal data for the recipient.

But the opposite case must also remain possible.

A service provider may receive information from which identifiers, quasi-identifiers and unnecessary granular attributes have already been removed or generalised; it may have no access to the source data, no key, no contractual entitlement to obtain identifying information, no operational channel allowing re-identification and no other reasonably available means of identifying the person.

In such circumstances, the fact that another entity remains capable of identifying the person should not, by itself, be attributed to the recipient.

That follows from the Court’s distinction between:

- the existence of identifying information somewhere; and
- the existence of **means reasonably likely to be used by the relevant entity**.

---

6. The anti-circumvention objective can be protected without inherited identifiability

The Guidelines justify paragraph 15 partly by the need to prevent controllers from circumventing the GDPR through outsourcing. This is a legitimate concern.

However, attributing the controller’s identifying capabilities to every entity acting on its behalf is not necessary to achieve that objective.

The controller does not cease to be subject to the GDPR merely because information disclosed to another entity is anonymous from that recipient’s perspective.

In *EDPS v SRB*, the Court itself demonstrated precisely this distinction. It held that the controller’s information obligations had to be assessed from the controller’s perspective and at

the time of collection, irrespective of whether the information subsequently became non-personal from Deloitte's perspective.

Accordingly:

> **the controller remains fully accountable for its own processing of personal data, including the transformation and disclosure;**

while

> **the status of the information in the hands of the recipient may be assessed separately.**

This protects data subjects without creating a legal fiction that an entity possesses identification capabilities which, in fact and in law, it does not possess.

---

7. The current rule may discourage privacy-enhancing architectures

The proposed rule could create an unintended disincentive to deploy strong data minimisation architectures.

Consider a controller that, before transmitting information to an external computing service, transforms:

> "Mario Rossi, born on 14 July 2009, residing at [address]"

into:

> "a person who was a minor at the relevant time".

Suppose that the external service receives:

- no name;
- no exact date of birth;
- no address;
- no case identifier;
- no persistent pseudonym;
- no other attribute allowing the person to be singled out or linked to external information;
- no access to the original dataset;
- no re-identification key;
- no contractual or practical means of obtaining identifying information.

The information may remain personal data for the originating controller because the controller can connect it with the underlying case.

But treating it automatically as personal data for the external service solely because that service performs computation on behalf of the controller removes much of the regulatory incentive for

precisely the kind of **data minimisation, generalisation and privacy-enhancing transformation** that the GDPR seeks to encourage.

A contextual identifiability test instead creates the correct incentive:

> **minimise more effectively, reduce linkability more effectively, and the legal consequences may change accordingly.**

---

8. Proposed amendment to paragraph 15

We propose replacing paragraph 15 with the following text:

> **15.** Where an entity processes information on behalf of another entity, the relationship between those entities is an important factor in determining the applicable perspective, but it should not by itself determine whether the information constitutes personal data for the processing entity.
>
> The assessment should consider whether the processing entity has, or may reasonably obtain or use, means enabling it to identify the individual, including through the controlling entity. Relevant factors may include technical access, contractual rights, operational practices, instructions, interfaces between the parties, the possibility of requesting additional information, and whether re-identification or re-linking forms part of the ordinary course of the processing.
>
> Where the processing entity does not possess and is not reasonably likely to obtain or use such means, and effective technical, organisational and, where appropriate, legal measures prevent access to identifying information, the fact that the controlling entity can identify the individual should not, by itself, result in the information being considered personal data for the processing entity.
>
> This assessment is without prejudice to the obligations of the controlling entity under the GDPR in respect of its own processing of personal data, including any processing undertaken to pseudonymise or anonymise the data and any subsequent disclosure of those data.

---

9. Proposed replacement for Example 3

We propose replacing Example 3 with the following:

> **Example 3: Processing on behalf of another entity**
>
> An online retailer wishes to use an external analytics provider. Before transmitting customer information, the retailer transforms the data by removing direct identifiers and generalising attributes that are not necessary for the analytics task.

> **Scenario A:** Under the service arrangement, the analytics provider can request customer-level information from the retailer where needed to verify results, or can otherwise obtain information allowing records to be linked back to identifiable customers. Those means may be reasonably likely to be used. The information should therefore be assessed as personal data from the analytics provider's perspective.
>
> **Scenario B:** The analytics provider receives only the transformed information. It has no access to the original records or to any re-identification key, has no contractual right or operational mechanism to obtain them, receives no persistent identifiers or other information enabling linkage, and technical and organisational measures prevent the retailer from providing identifying information as part of the service. If the provider has no other means reasonably likely to be used to identify the individuals, the information may be anonymous from the provider's perspective, even though it remains personal data from the retailer's perspective.
>
> In both scenarios, the retailer remains subject to the GDPR in relation to the personal data it processes and must ensure that the transformation and disclosure comply with its obligations under the Regulation.

---

10. Additional clarification on anti-circumvention

We also suggest adding the following clarification:

> **The Board may additionally clarify that arrangements designed merely to create an artificial separation of identifying information should not suffice. Where, in substance, the recipient can obtain or trigger access to identifying information in the ordinary course of the service, such information constitutes a means reasonably likely to be used and must be taken into account in the identifiability assessment.**

This would preserve the anti-circumvention objective without introducing a rule of automatic or inherited identifiability.

---

11. Relationship with the Digital Omnibus

The question is also currently before the Union legislature.

The Commission's Digital Omnibus proposal would make clear that information may not constitute personal data **for a given entity** where that entity does not have means reasonably likely to be used to identify the individual, even where another entity can do so.

The legislative proposal should not be treated as the legal basis for the interpretation proposed above. However, it demonstrates that this issue is currently subject to an active legislative policy choice.

For that reason, the Guidelines should be cautious about resolving through teleological interpretation a point that:

- was not decided by the Court in *EDPS v SRB*;
- was described by EDPB and EDPS themselves as an open question in February 2026; and
- is presently being considered by the Union legislature.

Source:
European Commission, Digital Omnibus, COM(2025) 837 final:
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2025:837:FIN

---

12. Conclusion

We therefore invite the EDPB to reconsider paragraph 15 and Example 3.

The relationship between a controller and an entity acting on its behalf should be treated as an important contextual factor when assessing identifiability, but not as a rule that automatically attributes the controller's identifying capabilities to the recipient.

The appropriate test should remain the one articulated by the Court of Justice, namely, in substance:

> whether the relevant entity has, or may reasonably obtain or use, means reasonably likely to identify the data subject.

Such an approach would:

- remain faithful to Article 4(1) GDPR and *EDPS v SRB*;
- preserve the GDPR obligations of the originating controller;
- prevent circumvention where re-identification remains realistically available;
- avoid circular reasoning around processor status;
- encourage stronger privacy-enhancing and data-minimisation architectures;
- provide incentives for controllers to disclose only the minimum information necessary for the relevant task.

References

1. Court of Justice of the European Union, Case C-413/23 P, *EDPS v SRB*
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0413

2. EDPB, Guidelines 02/2026 on Anonymisation, Version 1
   https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf

3. EDPB–EDPS Joint Opinion 2/2026 on the Digital Omnibus
   https://www.edpb.europa.eu/system/files/documents/2026-

02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf

4. European Commission, Digital Omnibus, COM(2025) 837 final https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2025:837:FIN

5. EDPB public consultation page — Guidelines 02/2026 on Anonymisation https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en