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

October 2026

Kasper Bjerre Hendrup Andersen, PhD

I welcome the EDPB's recognition that information need not be personal data for every entity and that anonymity does not require eliminating every conceivable identification risk.

These are important clarifications that reflect the contextual nature of the concept of personal data under Article 4(1) GDPR and Recital 26, as developed in the case law of the Court of Justice.

However, recognising these principles is only the starting point. Their practical value ultimately depends on how they are translated into a coherent legal methodology. In my view, certain aspects of the draft Guidelines risk introducing distinctions and assumptions that are difficult to reconcile with the structure of the GDPR and the Court's case law.

My observations therefore focus on three closely related questions: whose perspective should determine whether information constitutes personal data, how should that perspective operate in different relationships between actors, and which means of identification can legitimately be considered reasonably likely to be used?

The following comments identify the principal legal difficulties and propose targeted clarifications intended to strengthen the Guidelines' consistency, legal certainty and practical applicability.

I. Keep scope, roles and obligations distinct

Whether information concerns an identifiable person, which actor determines or performs its processing, and which obligations apply are connected but distinct questions. Articles 4(1), 4(7), 4(8), 26 and 28 must be read together with Recital 26, rather than allowing an assumed role to determine the scope of the Regulation.

EDPS v SRB confirms that pseudonymisation need not leave information personal for every recipient. It also assessed the controller's information obligation from its position at collection, rather than the recipient's subsequent situation. Neither a universal controller perspective nor a universal recipient perspective captures both findings. The judgment supports an actor-sensitive assessment of identifiability in the circumstances examined. It does not, however, establish that every GDPR obligation must invariably be assessed from the perspective of the entity physically holding the information. Anonymity for a recipient therefore does not erase the source controller's obligations regarding its own processing, anonymisation or disclosure.

For unidentified persons, the test is which means are reasonably likely to be used. It is neither a numerical probability threshold nor a requirement that identification be more likely than not. Information relating to an identified individual does not become anonymous merely because the processing entity has no intention of using the available identifiers.

II. Processor relationships: context, not automatic attribution

Paragraph 15 attributes the controller's perspective to a provider processing on its behalf, relying on prevention of circumvention and the complementary operation of contractual and statutory safeguards. These are legitimate objectives. However, Article 4(8) GDPR defines a processor by reference to the processing of personal data. The fact that a provider acts on another entity's instructions cannot, in itself, establish that the information constitutes personal data in the provider's hands.

An operation-based interpretation offers a more substantial justification: the provider may be performing part of an existing personal-data processing operation on behalf of the controller, even without being able to read the information. However, this interpretation still requires an explanation of why participation in that operation necessarily entails adopting the controller's identification capabilities, including where the provider has no reasonably available means of identification, directly or indirectly.

The distinction is important. The processing relationship may provide compelling evidence of realistic identification pathways, but it does not, without further legal justification, establish that every identification resource available to the controller must automatically be attributed to the provider. The Guidelines should therefore distinguish delegated personal-data processing from services confined to genuinely anonymous outputs, synthetic material or ancillary activities. Nor should automatic attribution be presented as an express holding of SRB.

My preferred approach treats the relationship as an objective circumstance within the provider's contextual assessment. Instructions, support access, screenshots, logs, supplementary information and the return of results for application to identifiable persons may establish realistic identification pathways. Restricted technical work without such pathways requires a different analysis. Neither encryption alone nor a promise not to identify decides the issue. The controller's perspective can be a practical shortcut in obvious cases without becoming the legal test for every boundary case.

A contextual approach leaves the source controller's obligations intact. Roles remain functional: parties cannot select them by contractual label or methodological freedom alone. Nevertheless, automatic attribution for instructed providers, contrasted with contextual assessment for independent recipients, may encourage restructuring rather than better safeguards. Confidentiality and security duties can remain meaningful without readable access; their desirability does not settle the scope question.

The need for clarification is expressly recognised in EDPB–EDPS Joint Opinion 2/2026, paragraph 19 and footnote 29. The Opinion records questions raised by stakeholders concerning whether recipients lacking independent means of identification may nevertheless qualify as processors or joint controllers. The EDPB and EDPS consider that such questions are better addressed through further EDPB guidance. The present Guidelines therefore provide an important opportunity to explain the legal foundations and limits of the respective approaches.

Proposed wording A | Paragraph 15

> *Where an entity processes information on behalf of another, the assessment of identifiability should take account of the actual processing operation and the legal and practical relationship between the parties. The controller's identification capabilities may be relevant, particularly where instructions, access arrangements, supplementary information, support procedures or the intended use of results establish reasonably likely means of identification.*

> *However, the existence of a processor relationship should not, without further legal justification, automatically entail the attribution of all identification capabilities available to the controller. The assessment should distinguish participation in an existing personal-data processing operation from the question of whether and why particular identification means may be attributed to the processor.*
>
> *This does not affect the controller's obligations concerning its own processing, anonymisation or disclosure.*

If automatic attribution is retained, explain its legal foundation, define the delegated operation, distinguish ancillary services and anonymous outputs, and address subprocessors and changes in service scope.

III. Joint controllership: determination without possession

The draft does not entirely omit joint controllership: paragraph 9 and footnote 7 expressly acknowledge it without access. What section 2.2 lacks is an operational explanation alongside entity-specific perspectives. Responsibility for jointly determining an upstream operation must be distinguished from receipt and separate use of its anonymised output. Neither question automatically answers the other.

Articles 4(7) and 26 concern joint determination of purposes and means, not shared possession. Wirtschaftsakademie distinguishes statistics received by the administrator from the underlying personal-data processing. Jehovan todistajat likewise rejects access as a prerequisite. Fashion ID concerns collection and transmission through the Like button, not receipt of Insights data; possible joint responsibility is confined to operations the operator helped determine.

EDPB Guidelines 07/2020, paragraphs 56-58, expressly recognise responsibility without access and its operation-specific limits. The Danish DMI decision similarly concerns advertising-related collection and transmission, not Google's subsequent independently determined processing.

My recommended interpretation is that, where the jointly determined operation involves personal data because one participating controller has relevant identification means, another participant's inability independently to identify does not exclude joint responsibility for that operation. This is not a claim that the Court has articulated a general doctrine pooling every cooperating entity's resources. Joint determination must actually exist; responsibility cannot spread automatically across the processing chain; genuinely anonymous outputs require separate assessment in distinct subsequent operations.

Differentiated responsibility does not displace Articles 26(3) and 82. Nor does the distinction rest on an assumption that joint controllers and processors must necessarily be subject to different identifiability standards. Rather, the case law expressly recognises joint determination without access, whereas the legal basis for automatically attributing a controller's identification capabilities to a processor requires further explanation. The Guidelines should articulate how these propositions can be reconciled, including whether and to what extent analogous operation-based reasoning applies to processors. The joint-controller judgments do not themselves settle that issue.

Proposed wording B | Paragraph 9 and section 2.2

> *An entity may qualify as a joint controller of a personal-data processing operation without receiving the information or possessing independent means of identifying the individuals concerned.*

> *Where two or more entities jointly determine the purposes and essential means of an operation involving personal data, the absence of independent identification capabilities on the part of one participant does not, in itself, exclude joint controllership for that operation.*
>
> *Joint responsibility must nevertheless be assessed in relation to the specific operations jointly determined. It does not automatically extend to subsequent processing independently determined by another entity or to the separate use of information that is anonymous in the circumstances of that subsequent processing.*

IV. Reasonably likely means: require a concrete pathway

Breyer requires examination of the means of combining information, including legal channels, and recognises legal prohibitions and disproportionate effort as grounds for identification risk being insignificant in reality. OC v Commission reaffirms that framework. Neither requires actual identification.

The draft rightly recognises insignificant risk, whole-chain assessment and objective factors in paragraphs 22 and 28-29. Paragraph 31 also recognises identification's value and associated risks while warning against relying on declared lack of motivation. The difficulty is consistent application, not absence of these principles. Available tools or supplementary data somewhere in the world do not establish a complete identification route. Conversely, an accessible and effective route is not excluded merely because its holder promises not to use it.

Paragraph 21's formulation that capabilities cannot be ruled out has a basis in SRB, paragraph 85. It should nevertheless remain tied to a concrete transfer and identification scenario, not unspecified recipients with unknown capabilities. Foreseeable future access can matter; completed transfers are not required. Mere inability to exclude unknown capabilities must not replace the assessment of reasonably likely means.

Require an evidence-based assessment of the relevant actor and operation, the reasonably foreseeable identification pathway, its legal, technical, organisational and economic conditions, and its timeframe. A concrete pathway does not require proof of an intended or fully specified sequence of identification steps. It requires sufficiently identifiable factual circumstances to support a reasoned conclusion that the relevant means, considered together, are reasonably likely to be used. The pathway should be assessed as a whole, including dependencies and safeguards, rather than treating each conceivable link as proof of the complete chain. No mathematical multiplication of probabilities is required.

Proposed wording C | Paragraphs 21 and 28-30

> *The assessment of reasonably likely means of identification should consider the relevant actor, the processing context and any sufficiently foreseeable circumstances in which the information may be combined with supplementary identification resources.*
>
> *Onward disclosure, third-party access or future technical capabilities should be taken into account where sufficiently identifiable objective circumstances support a reasonable expectation that the relevant identification means may become available and be used.*
>
> *The assessment should consider the identification pathway as a whole, including its technical feasibility, legal conditions, organisational arrangements, costs, required effort and relevant safeguards. It does not require proof of actual identification, an intention to identify or a fully specified sequence of identification steps.*

> *The mere inability to exclude the hypothetical capabilities of unspecified recipients should not, by itself, establish that identification is reasonably likely.*

V. Give statutory prohibitions substantive effect

The Court's reasoning in Breyer, paragraph 46, subsequently reflected in OC, paragraph 51, and SRB, paragraph 82, gives statutory prohibitions a substantive role in the assessment of identifiability. A legal prohibition should therefore not be treated merely as one cost or inconvenience among others. Advocate General Campos Sánchez-Bordona expressed a more categorical view in paragraph 73 of his Opinion in Breyer, stating that reasonable means of access must, by definition, be lawful. That Opinion supports the interpretation advanced here but must be distinguished from the Court's binding judgment.

Paragraphs 32–33 of the draft recognise the significance of legal prohibitions but allow the general assumption of lawful conduct to be rebutted where there is sufficient evidence of a concrete risk of unlawful identification. The difficulty is not necessarily the recognition of exceptional circumstances. It is the absence of a sufficiently clear explanation of when, and on what legal basis, the possibility of unlawful conduct may overcome an otherwise applicable statutory prohibition.

Although paragraph 33 identifies several potentially relevant objective factors, it remains unclear how these factors should be weighed and what connection they must have to a reasonably foreseeable identification pathway. Evidence of weak enforcement, potential financial gain or the general prevalence of criminal conduct does not, without more, establish that prohibited identification means are reasonably likely to be used by the relevant actor. Such a conclusion requires a sufficiently concrete identification pathway and an explanation of the relevance of the applicable legal restrictions.

Danish criminal law illustrates the importance of examining the specific identification pathway. Depending on the circumstances, unauthorised disclosure or use of confidential information by a public official may fall within section 152 of the Danish Criminal Code, while unauthorised access to a data system may fall within section 263. Sections 152a–152e extend or qualify the protection in specified circumstances, and section 155 may also be relevant to certain abuses of public office. These provisions have different elements and scopes of application. A breach of an internal instruction is not necessarily a criminal offence, and the existence of a criminal prohibition must be established for the particular route under consideration.

If matching information is segregated in a municipal system, a proposed route requiring unlawful disclosure or unauthorised entry cannot simply treat that information as available. The statutory barrier and any alternative lawful route must be assessed. Domestic criminalisation does not establish effectiveness against every foreign actor.

Three situations must remain distinct: hypothetical misconduct without a concrete pathway; demonstrated access risks, such as compromised credentials or an operative illicit disclosure arrangement; and identifying information already accessible after a breach. The first cannot automatically override a statutory barrier. The second requires an explanation of its legal relevance to the particular actor. The third requires reassessment of genuinely changed circumstances.

Proposed wording D | Paragraphs 32-33

> *An applicable statutory prohibition constitutes a substantive legal barrier that must be given appropriate weight when assessing whether particular means of identification are reasonably likely to be used.*

A hypothetical possibility of unlawful access, disclosure or identification does not, in itself, justify disregarding that prohibition. Nor should the potential economic or other benefit of unlawful conduct alone be sufficient to establish that prohibited identification means are reasonably likely to be used.

Where concrete circumstances nevertheless support the inclusion of an identification pathway involving prohibited conduct, the assessment should identify the relevant actor, the applicable legal prohibition, the objective circumstances supporting the anticipated conduct and the legal reasoning for treating that pathway as reasonably likely.

Alternative lawful means of identification and situations in which identifying information has already become realistically available following unlawful conduct must be assessed separately.

VI. Separate precaution from the legal threshold

Paragraph 89 recognises that appropriate security controls may restrict reasonably likely access to authorised users. Example 22 nevertheless includes accidental recipients and malicious actors among the potentially relevant entities, based on a precautionary assumption that the dataset could eventually be leaked despite strong safeguards.

Importantly, the example ultimately concludes that the No Linkage criterion is satisfied because the identified actors lack reasonably likely means of linking the data to identifiable individuals. The concern is therefore not the example's conclusion, but the preceding assumption that potential access through leakage or hacking may be treated as reasonably likely without a sufficiently explicit assessment of the relevant access pathway.

The Guidelines should distinguish the precautionary identification of potential recipients from the legal assessment of whether access to the data and subsequent identification are reasonably likely in the circumstances. The mere possibility of a security breach does not establish that either step is reasonably likely. Where a hypothetical access scenario is included in the legal assessment, the objective circumstances supporting that inclusion should be explained.

Security and identifiability assessments may share relevant evidence, but a precautionary threat model does not automatically determine whether information constitutes personal data under Article 4(1) GDPR.

Proposed wording E | Paragraph 89 and Example 22

The assessment of reasonably likely means of identification should distinguish between the likelihood of obtaining access to information and the likelihood of identifying individuals once access has been obtained.

The residual possibility of unauthorised access, accidental disclosure or security breaches does not, in itself, establish that identification is reasonably likely. The assessment should consider the combined pathway, including the relevant actors, the effectiveness of applicable safeguards, the availability of supplementary information and any relevant legal prohibitions.

Precautionary assumptions adopted for information security or risk-management purposes should be distinguished from legal conclusions concerning identifiability under Article 4(1) GDPR. Where such assumptions are relied upon to establish identifiability, the objective circumstances supporting that conclusion should be explained.

Anonymity is contextual but should not be judged with hindsight. A later event may expose an overlooked foreseeable pathway or create a genuinely new one. Reviews should reflect the data's lifecycle, changed access, compromised safeguards and reasonably foreseeable technical developments, not an indefinite assumption that every safeguard eventually fails.

Proposed wording F | Paragraphs 35, 42 and 88

> *The assessment of identifiability should be based on the circumstances existing at the relevant time, together with developments that are reasonably foreseeable during the anticipated processing or availability of the information.*
>
> *Material changes in technical capabilities, access arrangements, supplementary information or the effectiveness of safeguards may require reassessment. However, the subsequent emergence of an identification possibility does not, in itself, establish that an earlier anonymisation assessment was incorrect.*
>
> *A distinction should be made between identification pathways that were reasonably foreseeable at the time of the original assessment and genuinely new circumstances arising subsequently.*
>
> *The assessment should document its material assumptions, relevant safeguards, identified uncertainties and circumstances that would trigger reassessment. It should not require proof that identification will remain impossible under every conceivable future scenario.*

Retain the qualifications that the simplified approach is voluntary and failure of a technical criterion does not automatically establish personal data. Documentation should support the contextual conclusion, not prove universal impossibility. Challenges should identify the disputed pathway and supporting facts, without changing applicable procedural rules on proof.

Conclusion

The final Guidelines should preserve the protective purpose of the GDPR while ensuring that the assessment of identifiability remains legally coherent, context-sensitive and grounded in objectively relevant circumstances.

In particular, the Guidelines should clarify the relationship between the personal-data concept and the allocation of controller and processor responsibilities, explain how identification capabilities are assessed in different processing relationships, and provide a more precise account of the significance of statutory prohibitions and foreseeable identification risks.

The proposed amendments are intended to strengthen legal certainty without diminishing the obligations of controllers or the protection afforded to data subjects. I respectfully invite the Board to consider these clarifications when finalising the Guidelines.