October 2026

Cisco Response to the EDPB consultation on Guidelines 02/2026 on Anonymization

INTRODUCTION

Cisco welcomes the EDPB's initiative to update the framework for assessing anonymisation and supports the draft Guidelines' recognition that identifiability is contextual and may vary between entities.[1] [2] [3] [4] Cisco also welcomes the confirmation that anonymisation does not require a zero risk of identification, but rather an assessment of whether identification is reasonably likely in practice.[5] This practical standard is essential for enterprise technology services, where data protection often depends on layered controls, role separation, encryption, access restrictions and customer-specific governance rather than on the complete absence of any theoretical re-identification possibility.[6]

Cisco provides cloud, security and collaboration services that help organisations operate securely in managed enterprise environments. In many cases, customers provide data that has been pseudonymised, encrypted or otherwise protected, while retaining identifying information or cryptographic keys themselves. Cisco's technical, organisational and legal position differs materially from that of entities that use pseudonymous identifiers to link individuals across contexts, create profiles or otherwise distinguish and treat them differently, as illustrated by Example 6 of the draft Guidelines.[7]

The submission addresses four connected issues:

1. the need for coherence with the ongoing Digital Omnibus legislative process and other parallel EU initiatives addressing identifiability and pseudonymised data;
2. the need to keep the "means reasonably likely to be used" test grounded in realistic and evidenced re-identification pathways;
3. the need to avoid a categorical application of the controller's perspective to all processing entities, irrespective of their actual capabilities; and
4. the need to give appropriate weight to contractual safeguards as part of a layered technical, organisational and legal control framework.

1. The Guidelines should not pre-empt the Digital Omnibus and should support a coherent EU standard

The consultation takes place while the Digital Omnibus legislative process is considering issues that directly overlap with the draft Guidelines, including the definition of personal data, the entity-relative assessment of identifiability and the circumstances in which pseudonymised data may no longer be personal data for a particular entity.[8] The Commission's original proposal expressly confirms that information should not become personal data for a given entity merely because another entity, or a potential subsequent recipient, has means

[1] European Data Protection Board (EDPB), Guidelines 02/2026 on Anonymisation, Version 1.0, adopted 7 July 2026 ("Draft Guidelines").
[2] Regulation (EU) 2016/679 (GDPR), art 4(1) and recital 26.
[3] Case C-582/14, *Breyer v Bundesrepublik Deutschland*, EU:C:2016:779, paras 41-46.
[4] Case C-413/23 P, *European Data Protection Supervisor v Single Resolution Board*, EU:C:2025:645
[5] GDPR, recital 26; Breyer, C-582/14, paras 41-46.
[6] Draft Guidelines, paras 21-22; Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, adopted 10 April 2014, pp. 8-11 and 20-23.
[7] Draft Guidelines, Example 6.
[8] European Commission. (2025, November 19). Proposal for a regulation of the European Parliament and of the Council on the simplification of the digital legislative framework (Digital Omnibus) [COM(2025) 837 final] relevant proposed GDPR amendments; *Breyer*, paras 41-46; *EDPS v SRB*

reasonably likely to identify the individual.[9] The Council's consideration of a specific rule for processing on behalf of a controller further demonstrates that the application of these principles to controlled service relationships remains an active legislative question.[10]

The EDPB should avoid adopting guidance that could be read as settling questions that remain under active legislative consideration before that process has concluded. In particular, paragraph 15 establishes a categorical rule under which information that is personal data for a controller is necessarily personal data for an entity processing on the controller's behalf.[11] That approach goes beyond the Commission's original entity-relative formulation and is now the subject of express discussion in the Council's ongoing consideration of the Digital Omnibus.

The practical distinction matters.[12] A recipient that receives a rich dataset, has access to identifying information and uses pseudonymous identifiers to link individuals across services or contexts is in a fundamentally different position from a cloud, security or collaboration provider that:

- receives only a limited dataset;
- does not hold the additional information or keys needed to identify individuals;
- processes the data in a segregated customer environment;
- is subject to technical controls that prevent or materially restrict its ability to combine the data with other datasets;
- is contractually and organisationally restricted to delivering a defined service.[13]

The final Guidelines should allow this difference in capability and use to be reflected in the assessment. Otherwise, the entity-relative approach recognised in the Guidelines and in *EDPS v SRB* risks having limited practical effect.[14]

The response recommends that the EDPB:

- coordinate with the Commission and other relevant institutions to support a single, GDPR-consistent standard of anonymisation and identifiability across the GDPR, DMA, Data Act, Digital Omnibus and related EU instruments;[15]
- confirm that the contextual approach is the legal test and that it requires an assessment of the relevant entity's actual capabilities and circumstances;
- avoid categorical language that determines the status of data in a recipient's hands solely by reference to the controller's perspective;
- ensure that the final Guidelines do not pre-empt the outcome of the ongoing legislative discussion on the application of the entity-relative test to entities processing on behalf of a controller;[16] and
- commit to reviewing the Guidelines once the Digital Omnibus process has concluded.

[9] European Commission, *Digital Omnibus* proposal [COM(2025) 837 final], proposed amendment to GDPR art 4 and/or relevant recitals
[10] Council of the European Union, *Presidency revised compromise text on Digital Omnibus*, Council doc. 13112/26, 21 September 2026, 2025/0360(COD) (working version; not adopted).
[11] Draft Guidelines, para 15; GDPR, arts 4(7)–(8) and 28.
[12] *Breyer*, paras 41–46; *EDPS v SRB*
[13] GDPR, arts 24, 25, 28 and 32; EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted 7 July 2021, sections 4–6; GDPR, art 32(1)(a).
[14] Draft Guidelines; *EDPS v SRB*.
[15] Digital Markets Act, Regulation (EU) 2022/1925; Data Act, Regulation (EU) 2023/2854; European Commission, *Digital Omnibus* proposal [COM(2025) 837 final]; Council of the European Union, *Presidency revised compromise text on Digital Omnibus*, Council doc. 13112/26, 21 September 2026, 2025/0360(COD) (working version; not adopted).
[16] European Commission, *Digital Omnibus* proposal [COM(2025) 837 final]; Council of the European Union, *Presidency revised compromise text on Digital Omnibus*, Council doc. 13112/26, 21 September 2026, 2025/0360(COD) (working version; not adopted).

2. The "means reasonably likely to be used" test must remain realistic, proportionate and capable of being applied through recognised assurance mechanisms

The Guidelines correctly state that anonymity does not require the likelihood of identification to be reduced to zero; the risk must be insignificant in reality.[17] However, the combined effect of paragraphs 21, 28 and 30 risks being understood as requiring organisations to investigate re-identification possibilities across an indeterminate chain of recipients, onward recipients, public data sources and malicious actors, even where those actors do not have a concrete and realistic path to receive the data or successfully re-identify an individual.[18]

This should not be interpreted as requiring controllers, processors or sub-processors to conduct independent and recursive investigations of the datasets, systems, security vulnerabilities, onward recipients or future technical capabilities of every entity that could conceivably obtain the data. Such information will often be outside the assessing entity's visibility and control and cannot reliably be independently verified.[19]

The GDPR already provides a governance framework for processing chains, including the controller's accountability obligations, Article 28 processor and sub-processor arrangements, technical and organisational measures, and transparency obligations.[20] The final Guidelines should build on that framework and should not, through the anonymisation assessment, create an additional and unstandardised downstream due-diligence expectation.[21]

A broadly framed downstream investigation would be inconsistent, costly and unreliable. Different organisations could reach different conclusions regarding the same service provider or recipient based on incomplete or non-comparable evidence. It would risk reproducing some of the practical difficulties associated with transfer impact assessments: repeated, bespoke assessments of matters outside the assessing entity's visibility or control, without common evidence standards or reliable mechanisms for verification.

The relevant question should be whether a defined and realistically relevant entity has a practical pathway to access the data, obtain the necessary auxiliary information, apply a viable technique and successfully re-identify an individual.[22] For a controlled processing chain, the assessment should focus first on the direct recipient and be grounded in information reasonably available to the assessing entity, together with recognised, independently verifiable assurance evidence regarding relevant downstream safeguards.[23]

This approach is also consistent with the Commission's original Digital Omnibus proposal, which provides that information does not become personal data for a given entity merely because a potential subsequent recipient has means reasonably likely to identify the individual.[24] The final Guidelines should reflect that distinction by focusing on actual or realistically foreseeable disclosures and re-identification pathways, rather than speculative possibilities involving an indeterminate chain of later recipients.[25]

Such evidence should avoid the need for routine bespoke technical investigation of downstream entities, while not displacing consideration of concrete and realistic onward-access and re-identification pathways.

---

[17] Draft Guidelines, paras 21–22; GDPR, recital 26.
[18] GDPR, recital 26; *Breyer*, paras 41–46; WP29 Opinion 05/2014, pp. 8–11.
[19] GDPR, arts 28 and 32; EDPB, *Guidelines 07/2020*, sections 4–6; EDPB, *Recommendations 01/2020 on measures that supplement transfer tools*, Version 2.0, adopted 18 June 2021.
[20] GDPR, arts 5(2), 24, 28 and 32.
[21] EDPB, *Recommendations 01/2020*, Version 2.0.
[22] GDPR, recital 26; *Breyer*, paras 41–46; WP29 Opinion 05/2014, pp. 8–11; EDPB, *Guidelines 01/2025 on Pseudonymisation*
[23] GDPR, art 28; arts 40 and 42; EDPB, *Guidelines 1/2018 on certification*, Version 3.0, adopted 4 June 2019.
[24] European Commission, *Digital Omnibus* proposal [COM(2025) 837 final], proposed amendment to GDPR art 4 and/or relevant recitals
[25] GDPR, recital 26; *Breyer*, paras 41–46; WP29 Opinion 05/2014, pp. 8–11.

The final Guidelines should require a holistic, two-directional assessment that weighs factors increasing realistic identifiability against factors reducing it, including actual access conditions, availability and quality of auxiliary data, the resources and accuracy required for re-identification, and applicable technical, organisational and contractual safeguards.[26]

The following clarifications are recommended:

- an onward recipient should be assessed only where there is a concrete and realistic pathway by which it is likely to receive the data and has means reasonably likely to enable successful re-identification;
- the mere existence of publicly available information, remote onward-transfer possibilities, rogue employees, hackers, accidental disclosure risks or future technological developments does not itself make identification reasonably likely;[27]
- organisations should not be required to conduct bespoke, independent technical investigations of entities beyond their direct recipient, including investigations of their systems, datasets, security vulnerabilities, auxiliary-data holdings or onward processing arrangements;
- the assessment may rely on information reasonably available to the assessing entity and on recognised, independently verifiable assurance mechanisms, rather than requiring separate entity-by-entity investigation throughout the processing chain;
- existing GDPR governance mechanisms should be the primary means for managing controlled processing chains, including Article 28 contractual requirements, sub-processor authorisation and flow-down obligations, technical and organisational measures, approved codes of conduct, Article 42 certification and independent audit evidence.[28] These mechanisms should also be recognised as relevant evidence when assessing whether onward access, linkage or re-identification is realistically likely;
- where downstream safeguards need to be assessed, the Guidelines should permit reliance on standardised and independently verifiable mechanisms, such as approved codes of conduct, certification, Article 28 contractual arrangements supported by audit or assurance evidence, and comparable sectoral assurance frameworks, rather than bespoke entity-by-entity investigations;[29] and
- each entity that makes an onward disclosure should remain accountable for applying appropriate safeguards to that disclosure, based on the information and evidence reasonably available to it at the time. This does not require the original disclosing entity to repeat an independent technical assessment of every later recipient in a controlled processing chain.[30]

The EDPB should therefore provide a worked example of a controlled enterprise service chain, such as a cloud service involving authorised sub-processors. The example should show how a controller assesses its direct provider using the data actually disclosed, the provider's access model, Article 28 governance, technical controls, recognised assurance evidence and binding flow-down safeguards.[31] It should also confirm that the controller is not expected to conduct separate, bespoke technical re-identification assessments of every authorised sub-processor or remote onward recipient absent concrete evidence of a realistic onward-access and re-identification pathway.[32]

The Guidelines should require a rigorous, evidence-based assessment of realistic risks, while making clear that organisations are not expected to perform bespoke technical investigations of an indeterminate downstream ecosystem absent concrete facts indicating a realistic onward-access and re-identification

[26] GDPR, recital 26; WP29 Opinion 05/2014, pp. 8–11; GDPR, art 32.
[27] GDPR, recital 26; WP29 Opinion 05/2014, pp. 8–11; GDPR, arts 33–34.
[28] GDPR, arts 5(2), 24, 28, 32, 40 and 42.
[29] GDPR, art 28; arts 40 and 42; EDPB, *Guidelines 1/2018 on certification*; EDPB, *Recommendations 01/2020*.
[30] GDPR, arts 5(2), 24 and 28.
[31] GDPR, arts 28 and 32; arts 40 and 42.
[32] GDPR, recital 26; *Breyer*, paras 41–46; WP29 Opinion 05/2014, pp. 8–11.

pathway. Where downstream safeguards are relevant, the assessment should rely on existing GDPR governance arrangements and recognised, independently verifiable assurance mechanisms—not a new TIA-style due-diligence process requiring each organisation to investigate and validate every later recipient's systems, datasets and capabilities.[33]

3. Paragraph 15 should be reconsidered in light of the pending legislative clarification and should not disregard a processing entity's actual capabilities

Cisco recognises the important role of Article 28 GDPR in ensuring that controllers cannot avoid data protection obligations through outsourcing. However, paragraph 15 should not be interpreted or applied in a manner that makes the actual position of a processing entity irrelevant.[34]

The draft Guidelines state that where an entity processes information on behalf of a controller, the personal nature of the information should be assessed from the controller's perspective. The Commission's original Digital Omnibus proposal did not include an equivalent processor-specific rule, whereas the Council compromise proposes an express processor-specific rule.[35] The final Guidelines should therefore not treat paragraph 15 as resolving a legislative issue that remains under negotiation. At a minimum, they should explain how the controller–processor role allocation interacts with the entity-relative assessment of identifiability and the actual technical and organisational capabilities of the processing entity.[36]

At minimum, the Guidelines should distinguish between:

- an entity that can access identifying information, combine datasets or use pseudonymous identifiers to link individuals across contexts; and
- an enterprise service provider that receives only pseudonymised or encrypted data, does not hold the key or additional information needed to identify individuals, operates in a controlled environment and cannot use the data to attribute information to, profile or otherwise treat a particular person differently.[37]

This distinction is not based on a recipient's stated intentions.[38] It is based on the provider's architecture, access model, data segregation, key management, ability to combine datasets and actual technical capacity to identify an individual.[39]

Cisco does not suggest that an entity's contractual role alone determines whether data is personal data. Rather, the Guidelines should avoid treating a controller's ability to identify an individual as automatically establishing the same ability for every processing entity, regardless of the data and capabilities actually available to that entity.[40]

The EDPB is encouraged to:

- pending the conclusion of the Digital Omnibus process, clarify that paragraph 15 does not make a processing entity's actual technical and organisational capabilities irrelevant, and explain the significance of those capabilities for the application of the Guidelines;
- revise Example 3 to specify the data provided to the agency, the data and systems to which it has access, and the technical and contractual safeguards that apply;

[33] GDPR, arts 24, 28 and 32; arts 40 and 42; EDPB, *Recommendations 01/2020*.
[34] Draft Guidelines, para 15; *Breyer*, paras 41–46; *EDPS v SRB*; GDPR, art 28.
[35] European Commission, *Digital Omnibus* proposal [COM(2025) 837 final]; Council of the European Union, *Presidency revised compromise text on Digital Omnibus*, Council doc. 13112/26, 21 September 2026, 2025/0360(COD) (working version; not adopted).
[36] *Breyer*, paras 41–46; *EDPS v SRB*; GDPR, art 28; EDPB, *Guidelines 07/2020*, sections 4–6.
[37] *EDPS v SRB*; WP29 Opinion 05/2014, pp. 8–11; GDPR, art 32; EDPB, *Guidelines 01/2025 on Pseudonymisation*,
[38] *Breyer*, paras 41–46; *EDPS v SRB.*
[39] GDPR, recital 26; *Breyer*, paras 41–46; *EDPS v SRB*; EDPB, *Guidelines 01/2025 on Pseudonymisation*.
[40] *Breyer*, paras 41–46; *EDPS v SRB*; European Commission, *Digital Omnibus* proposal [COM(2025) 837 final].

- include a worked contextual example involving a service provider that receives pseudonymised data but has no access to the key or other identifying information;[41]
- distinguish providers that process data solely within a customer-controlled environment from recipients that use identifiers for cross-context linkage, profiling or individualised decision-making; and
- explain how the contextual assessment applies where a provider processes data that it cannot access in intelligible form due to encryption, key separation or comparable safeguards.[42]

4. Contractual safeguards should have meaningful weight as part of a layered control framework

Cisco agrees with paragraph 34 that contractual terms alone cannot make readily re-identifiable data anonymous.[43] Technical measures must do the primary work of reducing identifiability.[44]
However, paragraph 34 should not be read as discounting contractual safeguards in the assessment of means reasonably likely to be used. Once technical measures have reduced the practical ability to re-identify individuals, binding contractual and organisational restrictions may materially reduce the remaining likelihood that an authorised recipient will attempt or be able to identify individuals.[45]

This is also relevant to the assessment of controlled processing chains. Where an organisation relies on a direct provider that is subject to Article 28 governance, verified technical and organisational controls, and binding flow-down safeguards, those arrangements should be treated as relevant evidence when assessing whether onward access or re-identification is realistically likely.[46] They should ordinarily avoid the need for a separate, bespoke technical investigation of each entity further down the chain, while remaining subject to consideration of any concrete evidence of a realistic onward-access and re-identification pathway.

This is particularly important in enterprise service relationships. Article 28 terms are not merely commercial commitments.[47] They are part of the GDPR's accountability framework and are reinforced by obligations to process only on documented instructions, restrictions on sub-processing, audit and information rights, and the consequences that follow where a processor acts outside the controller's instructions.[48]

Contracts should be evaluated on their practical strength and operation. Relevant factors include whether they are supported by:

- a clear prohibition on re-identification, linkage and use of auxiliary data;
- defined purpose limitations and documented instructions;
- role-based access controls, logging and monitoring;
- segregation of customer environments and datasets;
- encryption, key separation or equivalent technical measures;
- audit rights and assurance mechanisms;
- notification, suspension, termination and liability provisions; and
- evidence of effective implementation and enforcement.[49]

The role of contractual safeguards will differ depending on the actor. They may materially affect what an authorised service provider is reasonably likely to do or be able to do. They will naturally carry less weight in relation to malicious or unauthorised actors, for whom technical and security measures are especially important.[50]

---

[41] EDPB, *Guidelines 01/2025 on Pseudonymisation*; GDPR, art 32; GDPR, art 32(1)(a).
[42] GDPR, art 32(1)(a); Draft Guidelines, paras 90–91.
[43] Draft Guidelines, para 34; WP29 Opinion 05/2014, pp. 20–23.
[44] WP29 Opinion 05/2014, pp. 20–23; GDPR, art 32.
[45] GDPR, recital 26; arts 24, 28 and 32.
[46] GDPR, arts 28 and 32; EDPB, *Guidelines 07/2020*; GDPR, arts 40 and 42.
[47] GDPR, art 28; EDPB, *Guidelines 07/2020*.
[48] GDPR, art 28(10); EDPB, *Guidelines 07/2020*.
[49] GDPR, arts 28, 32, 40 and 42.
[50] WP29 Opinion 05/2014, pp. 20–23; GDPR, art 32; GDPR, arts 33–34.

The following clarifications are recommended:

- clarify that contractual measures are relevant to the assessment of means reasonably likely to be used, particularly for authorised recipients;
- distinguish the role of contractual safeguards for authorised recipients from their more limited relevance to malicious or unauthorised actors;
- confirm that specific, enforceable, verifiable and monitored contractual restrictions should be weighed alongside technical and organisational measures when assessing residual risk;
- recognise that Article 28 arrangements should be assessed in light of their legal and operational role within the GDPR framework; and
- clarify in paragraph 91 that encryption, key separation and comparable measures may materially reduce the means available to a provider where it does not have access to the key and cryptanalysis is not reasonably likely.[51]

5. Practical guidance, assurance and proportionate reassessment

The Guidelines would benefit from practical tools that make the contextual approach reproducible and defensible without requiring bespoke downstream due diligence.[52] In particular, organisations need clearer guidance on the type and depth of information reasonably required for an assessment, the assurance evidence on which they may rely for controlled processing chains, how technical and contractual safeguards should be documented, and when reassessment is necessary.[53]

Cisco supports the use of recognised assurance evidence in a proportionate assessment. This may include relevant certifications, audit reports, approved codes of conduct, contractual commitments and summary-level evidence regarding categories of technical and organisational controls.[54] Such evidence should not eliminate the need for a contextual assessment of the direct recipient and realistic risk pathways. It should, however, be sufficient to avoid routine intrusive disclosure or independent validation of detailed security architectures, vulnerabilities or incident information relating to downstream entities.[55]

The following clarifications are recommended:

- provide a risk-based documentation template structured around the three criteria and the factors relevant to means reasonably likely to be used;
- recognise relevant assurance evidence, including certifications, audit reports, approved codes of conduct and independently verified control frameworks;[56]
- clarify that an assessment should not require intrusive testing of a recipient's systems or disclosure of detailed security-sensitive information absent a concrete reason to do so;[57]
- specify material reassessment triggers, such as broader release or access, a relevant security incident, new auxiliary data, a change in anonymisation technique, or a demonstrated development in re-identification capability;[58]
- confirm that reassessment should be proportionate to the nature of the data, access conditions and residual risk; and

[51] Draft Guidelines, para 91; GDPR, recital 26 and art 32(1)(a).
[52] GDPR, arts 24, 28 and 32; arts 40 and 42; EDPB, *Recommendations 01/2020*.
[53] Draft Guidelines, paras 35, 41 and 88; GDPR, arts 5(2), 24 and 25.
[54] GDPR, arts 28, 32, 40 and 42; EDPB, *Guidelines 1/2018 on certification*.
[55] GDPR, art 32; GDPR, arts 33-34.
[56] GDPR, arts 40 and 42; EDPB, *Guidelines 1/2018 on certification*.
[57] GDPR, recital 26 and art 32; GDPR, arts 33-34.
[58] GDPR, recital 26; WP29 Opinion 05/2014, pp. 8-11; GDPR, arts 5(2) and 24.

- develop worked examples for pseudonymised data, encryption and key separation, controlled enterprise processing environments, and onward transfers subject to technical, organisational and contractual restrictions.[59]

Conclusion

Cisco supports a rigorous and practical anonymisation framework that protects individuals while allowing organisations to use appropriately protected data responsibly. The final Guidelines should preserve the CJEU's contextual standard by focusing on realistic and evidenced re-identification pathways,[60] reflecting material differences between recipients' actual capabilities,[61] and giving due weight to layered technical, organisational and contractual safeguards.[62]

[59] GDPR, arts 28, 32, 40 and 42.
[60] GDPR, recital 26; *Breyer*, paras 41–46; WP29 Opinion 05/2014, pp. 8–11.
[61] *Breyer*, paras 41–46; *EDPS v SRB*, [insert pinpoint]; EDPB, *Guidelines 01/2025 on Pseudonymisation*.
[62] GDPR, arts 24, 28 and 32; GDPR, art 32(1)(a).

Annex: Priority drafting requests

Draft Guidelines provision	Cisco concern	Requested clarification or amendment
Paragraph 15; Example 3	The controller's perspective appears to determine the result categorically for a processing entity, regardless of its actual access and capabilities.	The Digital Omnibus legislative process is considering the relationship between the entity-relative identifiability test and processing on behalf of a controller. The final Guidelines should not prejudge that outcome. Pending legislative clarification, explain how a processing entity's actual technical and organisational position is relevant under paragraph 15; revise Example 3; and add a worked example involving pseudonymised data shared with a provider that lacks the key and additional information.
Paragraph 21	"Cannot be ruled out" is inconsistent with paragraph 22's "insignificant in reality" threshold.	Replace with a test of whether identification is reasonably likely in the circumstances.
Paragraphs 28–30, 89 and 92–93	The combined approach risks treating theoretical access to public data, malicious actors and future techniques as sufficient.	Require a realistic and evidenced pathway to access, auxiliary information, viable technique and successful identification.
Paragraphs 21, 28–30; footnote 21; paragraphs 89–90	The combined approach could be interpreted as requiring recursive, bespoke due diligence of sub-processors, onward recipients and other remote entities outside the assessing entity's visibility and control.	Confirm that organisations need not conduct independent technical investigations of entities beyond their direct recipient. For controlled processing chains, permit reliance on Article 28 governance, binding flow-down obligations, technical and organisational controls, approved codes of conduct, certification and independent assurance evidence, unless concrete evidence establishes a realistic onward-access and re-identification pathway.
Paragraph 30; footnote 25	The list of actors may be read as requiring routine analysis of all malicious or remote actors.	State in the operative text that actors are relevant only where their involvement is realistic on the facts.
Paragraphs 31 and 33	Accidental, negligent and unlawful conduct is potentially too broadly included.	Clarify that these factors matter where reasonably foreseeable and supported by contextual evidence of access and successful re-identification.
Paragraph 34	Contractual safeguards may be undervalued, including in controlled processing chains involving authorised providers and sub-processors.	Confirm that enforceable, verifiable and monitored contractual restrictions—especially Article 28 arrangements, flow-down obligations and restrictions on re-identification, linkage and onward disclosure—should be weighed alongside technical and organisational measures. They should be recognised as relevant assurance evidence when assessing whether downstream access or re-identification is realistically likely.

Paragraphs 90–91	The treatment of access restrictions and encryption needs further calibration.	Explain that, depending on their implementation and the recipient's realistic access and capabilities, encryption, key separation and controlled access may materially reduce available means where the recipient lacks key access and decryption is not reasonably likely.
Paragraphs 35, 41 and 88	Documentation and reassessment expectations are open-ended.	Provide risk-tiered documentation expectations, recognised assurance mechanisms and defined reassessment triggers.
Examples 3, 7, 9, 18 and 20	The examples lack facts necessary for organisations to apply the test.	Develop worked examples that identify the entity, data, access conditions, safeguards, realistic attack pathway and the factor that changes the conclusion.
Overall	The Guidelines overlap with pending Digital Omnibus work.	Coordinate with the Commission and relevant EU institutions to maintain a coherent standard. The final Guidelines should not prejudge the pending legislative outcome, particularly on entity-relative identifiability, potential subsequent recipients and the treatment of processing on behalf of a controller; commit to review the Guidelines following conclusion of the Digital Omnibus process.