Response to the EDPB public consultation on draft Guidelines 02/2026 on Anonymisation

We have taken a note of the European Data Protection Board's (EDPB) draft "Guidelines 02/2026 on Anonymisation" (Guidelines), which have been circulated for public consultation until 30th October, 2026. We are grateful for the opportunity to provide comments on the draft Guidelines.

Executive summary

We welcome the EDPB's efforts to provide a coherent framework for assessing anonymisation under the General Data Protection Regulation (GDPR). However, we regret to see that the draft Guidelines do not refer to the multistakeholder workshop held on 12 December 2025 on anonymisation and pseudonymization nor do they refer to the corresponding report published on 18 February 2026. The event was intended to support the EDPB's ongoing work, particularly the Guidelines on anonymisation. The draft Guidelines appear to have been drafted in isolation from the stakeholders input. The final Guidelines should better reflect how the spirit of the EDPB's Helsinki Statement has been implemented, particularly its principles on fundamental rights, SME compliance, competitiveness and responsible innovation. Moreover, we would like to point out the cross-industry letter[1] sent to the EDPB following the CJEU *EDPS v SRB* ruling where we asked the EDPB for practical guidance that would endorse the ruling and elaborate on how different industries can innovate responsibly while ensuring proper level of protection to the personal data. Current draft Guidelines do not address the requests raised in the letter leaving many industries without proper guidance on how to unlock the full potential of data in a safe way.

Nonetheless, we appreciate the fact that the draft Guidelines try to offer clarification, particularly by recognising that failing one anonymisation criterion presented by the EDPB does not necessarily mean that information is personal data. However, several aspects require refinement to ensure alignment with art. 4(1), recital 26 GDPR and the Court of Justice of the European Union (CJEU or Court) case law, while providing organisations with sufficient legal

[1]https://www.fedma.org/wp-content/uploads/2025/11/251117-Letter-to-EDPB-on-upcoming-stakeholder-event-on-anonymisation-and-pseudonymisation.pdf

certainty. In particular, the recognition of the relative nature of personal data – as confirmed by the CJEU in *EDPS v SRB* – should not be counteracted by an excessively broad interpretation of what constitutes means "reasonably likely to be used" for identification.

First, the final Guidelines should distinguish clearly between means that are objectively “reasonably likely to be used” and scenarios that are merely technically conceivable but unrealistic. The final Guidelines should also recognise foreseeability as an inherent component of the “reasonably likely to be used” assessment under recital 26 GDPR. The relevant question is not whether identification is theoretically possible, but whether identification is reasonably foreseeable (i.e. realistic) in the specific circumstances. Speculative attacks, unlawful access, accidental disclosure or hypothetical future capabilities should affect an anonymisation assessment only where objective, case-specific evidence demonstrates a concrete and non-insignificant likelihood of their occurrence. Treating every theoretical possibility as relevant would effectively transform the contextual approach into the more conservative "simplified" approach proposed by the EDPB and set a standard that is not aligned with the GDPR's own wording.

Second, the final Guidelines should distinguish consistently between isolating a unique record and identifying the natural person to whom it relates. “No Record Isolation”, “No Linkage” and “No Inference” are useful analytical and precautionary criteria, but they are not independent statutory conditions of anonymity. In particular, uniqueness as a rule does not amount to identification; instead, uniqueness can *contribute* to identification if its combination with additional data or circumstances enables a person to be operationally distinguished and treated differently through means reasonably likely to be used.

Third, paragraph 15 should not automatically attribute the controller’s identifiability perspective to every processor. The controller-processor relationship is highly relevant, and processing and sub-processing must not permit circumvention of the GDPR, but it should not replace a factual assessment of the legal, technical and organisational means available to the processor for each specific operation. Roles under the GDPR are functional and operation-specific. If the EDPB retains its proposed approach, it should explain its doctrinal basis, scope and limits, including its application to processors, sub-processors, independent processing activities and existing arrangements.

The final Guidelines should also give the contextual approach at least equal prominence to the simplified approach. The latter should be presented expressly as optional and no adverse inference should arise solely because an organisation instead relies on a properly reasoned and documented contextual assessment. Practical guidance tailored to Small and Medium enterprises (SMEs) and start-ups is particularly important, together with examples explaining how privacy-enhancing technologies (PETs) may contribute to anonymisation in appropriate circumstances.

Greater consistency with other areas of European Union (EU) digital regulation is also needed. The EDPB should address the apparent tension between the draft Guidelines and the European Commission's (Commission or EC) approach under art. 6(11) of the Digital Markets Act (DMA), particularly concerning the cumulative effect of technical alteration, access restrictions and contractual obligations.

Finally, the reassessment of anonymisation should be proportionate and risk-based. The final Guidelines should identify the responsible actors, relevant trigger events, appropriate review intervals and required documentation, while confirming that a subsequent change in circumstances does not retroactively invalidate a reasonable and properly documented original assessment. Where information later becomes identifiable, its reclassification as personal data should operate prospectively from the point at which the relevant entity knows, or reasonably ought to know, that the circumstances have materially changed.

These clarifications would preserve the GDPR's high level of protection while ensuring that the concept of anonymisation remains legally workable, technologically neutral and capable of supporting responsible data use and investment in privacy-enhancing innovation.

Areas of concern

- The draft Guidelines only rely on hypothetical use cases. The EDPB should consider examples from the report "From pseudonymous to anonymous data"[2] that compiles concrete, real-world and industry-driven use-cases on data pseudonymisation and anonymisation. The final Guidelines should be clear and accessible to a broad audience, including readers without specialist technical or legal expertise. Practical examples are

[2]https://cabinet-samman.com/wp-content/uploads/2026/06/From-Pseudonymised-to-Anonymous-Data-EU-Industry-Use-Cases-Joint-Policy-Report-2.pdf

essential to help anyone engaging with these issues understand the guidance and apply it in practice.

- The draft Guidelines appear to adopt an overly expansive approach to unlawful, malicious and hypothetical means of re-identification. While the draft Guidelines recognise that means prohibited by law may in certain circumstances be disregarded (see para. 89), other passages appear to require controllers to take into account speculative attacks (para. 30 and following), and a broad range of hypothetical bad actors even where effective safeguards are in place. This creates uncertainty as to the proper threshold for determining which means are "reasonably likely to be used" and risks turning the anonymisation assessment into an analysis of remote or merely theoretical possibilities such as cyber hacking (which can occur nowadays to any entity hence *de facto* excludes anonymisation opportunities for anyone). We recommend that the different sections are better aligned to reflect a risk-based approach.
- The draft Guidelines risk equating mere distinguishability with identification or identifiability of a natural person. While they initially recognise that identification requires both distinguishing an individual and making it possible to treat that individual differently, some examples appear to reduce this test to singling out alone. This may blur the distinction between identifying a device, record or person within a particular context and having a realistic ability to link information to that individual or direct a decision or consequence towards them.
- The draft Guidelines risk making the simplified approach a *de facto* default, despite recognising it as an optional and stricter assessment than the law requires. At the same time, the draft Guidelines present the contextual (i.e. relative) approach as very complex, potentially discouraging its use. This may turn a voluntary methodology, based on an assumption that data is personal by default, into a quasi-mandatory standard without clear legal basis, particularly in light of the relative approach endorsed by the CJEU in *EDPS vs SRB*[3] case.
- The draft Guidelines may impose a disproportionate practical burden on SMEs. The contextual approach requires complex legal and technical assessments, while the simplified approach may encourage SMEs to treat genuinely anonymous data as personal, reducing their potential to innovate.

[3] Court of Justice, judgment of 4 September 2025, *European Data Protection Supervisor v Single Resolution Board*, C-413/23 P, ECLI:EU:C:2025:645.

- The draft Guidelines risk attributing the controller's perspective on identifiability automatically to processors and sub-processors, even where they lack any realistic means of identifying individuals. Yet there remain questions as to the compatibility of this approach with the contextual or relative approach recognised by the CJEU in *EDPS vs SRB* judgment and based on the text of recital 26 and art. 4(1) GDPR.
- The draft Guidelines appear to take a stricter view of the role of technical and contractual safeguards than the European Commission in the Alphabet decision[4] under Article 6(11) of the DMA. While the EDPB stresses that encryption, access controls and contractual restrictions do not in themselves establish anonymity, the Commission gives such measures significant weight in treating the relevant dataset as anonymised. This divergence creates uncertainty as to how technical and contractual restrictions should affect the assessment of means "reasonably likely" to be used for re-identification.

Key recommendations

- The final Guidelines should ensure that the understanding of anonymisation aligns with current CJEU case law, in particular the *EDPS vs SRB* ruling, and the relevant provisions of the GDPR. The focus should be on the means that are realistically and reasonably likely to be used when it comes to assessing the anonymisation, not hypothetical ones. In other words, the final Guidelines should - in all its sections - focus on foreseeability, not mere theoretical possibility. This approach would enhance legal certainty and provide a stronger incentive for the adoption of anonymisation.
- The final Guidelines should acknowledge the relevance of anonymisation in the context of other EU digital legislation, including the Digital Markets Act (DMA), the Data Governance Act (DGA), the Data Act and the Artificial Intelligence Act (AI Act). To ensure regulatory coherence and legal certainty, the EDPB should consult with the relevant regulatory authorities when developing the final Guidelines, with a view to ensuring that their interpretation and application of anonymisation are consistent with, and operationally workable across various digital legislations. Such coordination would help avoid divergent interpretations, reduce compliance complexity for businesses and promote a consistent approach to anonymisation across the EU digital regulatory landscape.

[4] European Commission, *Case DMA.100209 SP Alphabet Article 6(11),* Decision of 16 July 2026.

- The final Guidelines should clarify that singling out, by itself, does not necessarily amount to identification. Whether a person is identifiable based on singling out should be assessed taking into account the broader context. Moreover, the EDPB should apply its two-step test to identifiability (i.e. (i) distinguishability and (ii) distinct treatment) consistently. Singling out tackles distinguishability, not distinct treatment.
- The final Guidelines should not determine from the outset that a processor is always under the umbrella of the relevant controller when it comes to assessing whether data processed on the controller's behalf constitutes personal data also for the processor. It appears too far-reaching, and to go against the *EDPS vs SRB* ruling, as the CJEU held there that there is a need for a case by case assessment (in a case where the recipient entity, Deloitte, appeared in fact to act as processor) and that an entity needs to have the means reasonably to be used to re-identify the data subject. Notably, situations of hybrid or dual use, i.e. where a processor processes the same set of data on behalf of the controller as well for its own purposes, raises questions regarding the nature of the data in question if that processor has no means of getting to identification. While information can be both personal data from one entity's perspective and anonymous data from another's perspective, it is difficult to conceive how it could have both natures from the same entity's perspective. The EDPB's position can moreover create issues for existing contracts that explicitly permit a processor to use data in an anonymous manner as a result of it not having any means of re-identification. A teleological application of the GDPR is important, but it cannot lead to inherent contradictions or impossible situations either. Paragraph 15 should therefore be reformulated so that the controller's perspective may be relevant, and in appropriate circumstances decisive, for processing carried out strictly on its behalf, but without establishing an irrebuttable rule applicable solely by virtue of the processor qualification. The assessment should remain tied to the specific processing operation, the applicable GDPR obligation, and the objective means reasonably likely to be used in the circumstances of the case.
- The final Guidelines should avoid suggesting that the simplified approach – under which anonymisation is more difficult to attain – is a better option than the contextual approach – which applies the principles set out by the CJEU. Maintaining the current wording in the final Guidelines would otherwise likely discourage organisations from attempting anonymisation in the first place, as it underlines the complexity of the contextual approach rather than promoting anonymisation.

- The EDPB should clarify in the final Guidelines the role that technical and contractual safeguards play in determining whether re-identification is “reasonably likely” within the meaning of the GDPR. The EDPB should clarify in the final Guidelines the role that technical and contractual safeguards play in determining whether re-identification is “reasonably likely” within the meaning of the GDPR. The EDPB's view differs from the European Commission’s approach in the Alphabet DMA decision creating divergent regulatory standards. This situation does not give organisations legal certainty regarding the assessment of whether data can reasonably be considered anonymous. Perhaps addressing this issue would be useful while writing the final Anonymisation Guidelines or the final Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation[5].
- The draft Guidelines should be reviewed to provide clearer, more actionable guidance and practical examples that organisations of all sizes and across all sectors can apply. Various organisations need workable guidance that reflects the realities of different processing contexts. The final Guidelines should address these diverse needs and provide concrete examples of how anonymisation can be achieved in practice. This would help organisations make effective use of anonymisation and unlock the potential of their data, benefiting data subjects and supporting innovation within the European Union.

1) Means reasonably likely to be used

The final Guidelines should draw a clearer distinction between means that are objectively “reasonably likely to be used” and scenarios that are merely technically conceivable. The concern is not that unlawful, malicious or accidental conduct can never be relevant, but that such conduct should form part of the contextual assessment only where the circumstances demonstrate a concrete and non-insignificant likelihood of its occurrence.

Paragraphs 32 - 33 recognise this by stating that compliance with the law may generally be presumed and that this presumption may be rebutted only by sufficient evidence of a concrete risk that unlawful means are nevertheless reasonably likely to be used. Paragraph 89 similarly states that, where appropriate confidentiality controls are in place, access constitutes a means reasonably likely to be used only by authorised users.

[5] European Data Protection Board and the European Commission- *Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation*.

However, Example 22 appears to apply a different threshold: although the data have not been publicly released and are protected by strong, state-of-the-art cybersecurity measures, the research institute assumes “out of caution” that a leak remains possible over a sufficiently long period and consequently treats hackers, accidental recipients and further downstream recipients as persons capable of accessing the data through means reasonably likely to be used. The EDPB should refrain from applying such a precautionary principle, which is inconsistent with the GDPR’s risk-based approach. The assessment should instead consider the actual likelihood of access in the specific circumstances, rather than treating the theoretical possibility of a future leak as sufficient. Although the Example 22 ultimately excludes persons possessing the contextual knowledge necessary for linkage and therefore does not automatically preclude a finding of anonymity, its reasoning at the access stage nevertheless appears to equate long-term possibility with reasonable likelihood. A similar ambiguity arises from the illustrative list in paragraph 30, which includes rogue employees, foreign intelligence services, unethical companies and cybercriminals, and from paragraph 91's reference to possible decryption without possession of the key. These passages should not be understood as requiring controllers to assess every conceivable hostile actor, future leak or theoretically possible attack. Such an interpretation would transform the contextual approach into the optional simplified approach, which the draft Guidelines themselves acknowledge may overestimate the likelihood that certain means will be used and may therefore go beyond the applicable legal standard. It would also be difficult to reconcile with recital 26 GDPR and the CJEU’s judgments in *Breyer*[6], *OC v Commission*[7] and *EDPS v SRB*, according to which a theoretical possibility is insufficient and persons or means are relevant only where they have, or may obtain, access to means reasonably likely to be used. Identification means may be disregarded where their use is prohibited by law or practically impossible because it would require disproportionate time, cost or labour, making the risk insignificant in reality. The *Scania*[8] and *IAB Europe*[9] CJEU judgements likewise concern concrete legal or practical channels connecting the relevant entity with the additional information, rather than purely hypothetical access. A useful comparative reference is

[6] Court of Justice, judgment of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.
[7] Court of Justice, judgment of 7 March 2024, *OC v European Commission*, C-479/22 P, ECLI:EU:C:2024:215.
[8] Court of Justice, judgment of 1 February 2024, *Scania AB and Others v European Commission,* C-251/22 P, ECLI:EU:C:2024:103.
[9] Court of Justice, judgment of 7 March 2024, IAB Europe v Gegevensbeschermingsautoriteit, C-604/22, ECLI:EU:C:2024:214.

the ICO's guidance on effective anonymisation[10], which recommends the "motivated intruder" test and expressly confirms its use by both the ICO and the First-tier Tribunal (General Regulatory Chamber). The test assesses whether a person motivated to identify individuals would be likely to succeed, taking into account their competence, available resources, investigative techniques and background knowledge, alongside the nature and value of the data and the safeguards in place. It requires a realistic assessment of the means reasonably likely to be used: specialist expertise or unlawful methods should also be considered where the circumstances make their use reasonably likely. The ICO expressly rejects the need to eliminate every hypothetical or theoretical possibility of identification. The EDPB should therefore clarify that speculative attacks and unauthorised or accidental access may be considered under the contextual approach only where objective, case-specific evidence establishes that they are reasonably likely. The final Guidelines should explain how a structured assessment, such as the motivated intruder test, can help organisations substantiate this likelihood in practice. In other words, the final text should recognise foreseeability as an inherent component of the "reasonably likely to be used" assessment under recital 26 GDPR. The relevant question is not whether identification is theoretically possible, but whether identification is reasonably foreseeable (i.e. realistic) in the specific circumstances. Absent such evidence, the mere possibility of certain means may be relevant under the simplified approach, but cannot prevent information from being regarded as anonymous under the GDPR.

2) Understanding of "singling" out in the context of identification

The draft Guidelines should distinguish more consistently between the uniqueness or isolation of a record and the identification of the natural person to whom that record relates. Paragraph 19 appears to establish a two-part test of identification - the person must be distinguishable from others within a given context, thereby making it possible to treat that person differently. Paragraphs 52 and 99 correctly preserve this distinction. Mere uniqueness should therefore trigger additional contextual assessment, rather than automatically establishing identifiability.

However, paragraphs 23-24 and Example 5 use language that appears to deviate from this analysis and to focus on uniqueness alone.

[10] Information Commissioner's Office, Anonymisation, "How do we ensure anonymisation is effective?", in particular the sections: "What is the 'motivated intruder' test?" and "How do we apply the motivated intruder test?"
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/how-do-we-ensure-anonymisation-is-effective/#applythemotivatedintrudertest

Paragraph 23 places an IP address alongside a name, social-security number and email address as an example of a single piece of unique data capable of identification, when in reality an IP address may identify only a device or network connection and does not necessarily distinguish the natural person using it (additional data being then needed to that end). This qualification is particularly important because *Breyer* CJEU judgment demonstrates that a dynamic IP address constitutes personal data from a particular entity's perspective only where that entity has means reasonably likely to be used to obtain the additional information necessary to identify the user.

Example 5 creates an ambiguity by concluding that the only person simultaneously wearing a black suit and walking a dog in live CCTV footage is identified, merely because that combination of visible attributes is unique within the street. In the context of live CCTV, the second element of the test might indeed be satisfied if the operator can select, follow, address, monitor or direct another individualised action towards that person. Yet Example 5 does not identify any such capability and therefore appears to treat the isolation of a visible figure as sufficient in itself. A description such as "the person in the black coat" may distinguish one figure within a scene, just as a unique combination of values may isolate one row within a dataset, but this should not automatically establish that the underlying natural person is identified or identifiable. The decisive distinction is between mere observational uniqueness and uniqueness that makes a natural person operationally distinguishable for individualised treatment through means reasonably likely to be used.

The EDPB should therefore align paragraphs 23-25 and Example 5 with other paragraphs by clarifying that the "No Record Isolation" violation triggers further contextual, linkage and inference analysis, but only where the isolated record can be connected to or used in relation to the natural person in a manner permitting differentiated treatment.

3) Attribution of the controller's perspective to processor

Paragraph 15 should be reformulated to distinguish between the factual identifiability of a natural person for a processor and the legal attribution of the controller's perspective to that processor for particular processing operations. The anti-circumvention objective invoked by the draft Guidelines is legitimate. We support the view that a controller cannot avoid its GDPR obligations merely by sub-processing an operation. However, paragraph 15 goes further by stating categorically that information which is personal for the controller must also be considered

personal for the processor, even where the processor has no means reasonably likely to be used to identify the individuals. Where the processor genuinely lacks any realistic means of identification (for example when PETs like Secure Multi-Party Computing or Trusted Execution Environments are deployed), this is not a factual conclusion reached by applying art. 4(1) and recital 26 GDPR, but a legal fiction based only on the processor's relationship with the controller.

The CJEU judgment in *EDPS vs SRB* case does not itself establish a general processor exception to relative identifiability. On the contrary, the CJEU held that information need not constitute personal data in all cases and for every entity, and that technical and organisational measures may make the information non-personal for a recipient that cannot identify the data subjects (paragraphs 75-87). The Court separately held that the SRB's transparency obligation had to be assessed from the SRB's perspective at the time when the data were collected. This reasoning preserved the controller's pre-existing information obligation irrespective of the status of the data in the recipient's hands. It did not determine the status of an instruction-bound processor under the GDPR, establish permanent attribution of the controller's perspective across all subsequent operations or sub-processing levels, or hold that a recipient's own factual perspective becomes irrelevant whenever it has a contractual relationship with the sender. Paragraph 15 should therefore be presented as an additional teleological interpretation adopted by the EDPB, rather than as a result already settled by the CJEU.

The existence of a controller-processor relationship should therefore be treated as a highly **relevant factual circumstance in the identifiability assessment, rather than as a conclusive substitute for that assessment.** This would also be consistent with paragraph 13 of the draft Guidelines, which identifies the relationship between the parties and the fact that one entity may process information on behalf of another among the circumstances relevant to determining the applicable perspective.

Moreover, the proposed rule risks conflating two legally distinct questions - whether information constitutes personal data from the perspective relevant to a particular processing operation and whether an entity acts as controller or processor in respect of that operation. The latter is itself a functional and fact-dependent classification. The EDPB has consistently stated in Guidelines 07/2020[11] that controller and processor are functional concepts allocating responsibilities

[11] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*.

according to the parties' actual roles, that their classification follows from factual circumstances rather than contractual designation.

Using the entity's status as a processor to determine conclusively that the information must constitute personal data for that entity therefore risks introducing circular reasoning. Under art. 4(8) GDPR, a processor is itself defined as an entity which "processes personal data on behalf of the controller". The existence of processing "on behalf of" another entity may be highly relevant to whether means of identification available to that other entity are reasonably likely to become available to the processing entity, but it should not eliminate the need to examine the actual and reasonable legal, technical and organisational circumstances.

This distinction is particularly important where technical and organisational measures effectively prevent the processing entity from identifying the individuals concerned. In the *EDPS vs SRB* case, the Court held that such measures may result in information not being personal in nature for an entity receiving pseudonymised data, and recalled that means of identification are not "reasonably likely to be used" where identification is prohibited by law, impossible in practice, or would require disproportionate effort.

The EDPB's concern that controllers should not be able to circumvent the GDPR by sub-processing is relevant. However, continuity of the controller's obligations and accountability should not be equated with an automatic attribution of the controller's identifiability perspective to the processor. The Court itself adopted a more targeted approach in *EDPS vs SRB* - for the information obligation at issue, it held that identifiability had to be assessed from the controller's perspective because of the nature, timing and purpose of that specific obligation, while expressly leaving open whether the information was personal data from the perspective of the recipient, Deloitte (who appears to have been a processor), after its transfer (paragraphs 110 - 113 *EDPS vs SRB* case).

Leaving paragraph 15 in its current form risks creating a regulatory asymmetry whose rationale and practical implications should be clarified. A processor acting strictly on the controller's instructions would have to treat the data as personal based on the controller's perspective, even where it has no realistic means of identifying the individuals. By contrast, an independent recipient, or the same entity acting independently in relation to a separate operation, could potentially assess the same data as anonymous from its own perspective.

Moreover, paragraph 15 may have significant consequences for existing arrangements and investments in privacy-preserving technologies. A categorical rule requiring the controller's perspective to be applied to processors could therefore materially alter the compliance assumptions on which such arrangements were designed. It may also undermine regulatory predictability for parties that structured their arrangements in good faith on the basis of a recipient-specific assessment of identifiability. Although the (draft) Guidelines are not legally binding, they are likely to have considerable practical influence on the interpretation and enforcement of the GDPR by national data protection authorities and national courts. Paragraph 15 should be changed or at least significantly clarified when it comes to its application to the existing processing arrangements.

The final Guidelines should therefore abandon such a strict approach and instead focus more on explaining when the controller's perspective might be relevant for the processor and/if for sub-processor chains while assessing the identifiability and means reasonably to be used. If the EDPB wishes to maintain this approach, the final Guidelines should explain its doctrinal basis, purpose and limits instead of justifying it solely on the teleological interpretation of the GDPR for the addressees of the Guidelines to have a better understanding on why the EDPB assumes it is appropriate to create a certain legal fiction that is not based on the case law nor on the text of the law itself.

4) Practical challenges for organisations to apply the Guidelines

The draft Guidelines correctly explain that the contextual approach reflects the legal standard for anonymisation, while the simplified approach may go beyond that standard. Paragraph 48 and footnote 36 appropriately acknowledge that the simplified approach may result in anonymous information being treated as personal data and that it cannot be relied upon by third parties to establish that information is personal or that a controller has infringed the GDPR. These are important and welcome safeguards.

Nevertheless, the practical presentation of the two approaches may give the impression that the simplified approach is the preferred route. Paragraph 48 introduces an unnecessary precautionary standard that goes beyond the GDPR's risk-based approach. Applying the GDPR "in case of doubt" undermines legal certainty and may lead organisations to incur unnecessary compliance costs. It also restricts the unlocking of data that can be used for data and AI led

innovation. Additionally, paragraph 49 suggests that controllers may begin by considering whether re-identification is possible in theory, while paragraph 53 explains the three anonymisation criteria primarily through the simplified approach. At the same time, the contextual approach is described as complex and as presenting a risk of incorrect conclusions where relevant contextual elements are not known. Organisations may therefore understand the simplified approach as the approach generally expected by data protection authorities, even though it is intended only as an optional and more conservative assessment method. This could, in practice, blur the distinction between a precautionary screening tool and the legal test arising from art. 4(1) and recital 26 GDPR, as interpreted by the CJEU in *EDPS vs SRB* case.

This issue is particularly relevant for any company, which may have limited access to the specialist legal and technical expertise required to identify all relevant actors, auxiliary datasets, possible re-identification chains and evolving technical capabilities. While the simplified approach may appear more manageable, its systematic use could lead many organisations to classify genuinely anonymous information as personal data, thereby reducing the practical benefits of anonymisation and potentially discouraging investment in privacy-protective innovation. Conversely, the contextual approach may require resources and documentation that are disproportionately burdensome for smaller organisations. The final Guidelines would therefore benefit from SMEs-focused examples and practical guidance showing how a robust contextual assessment can be performed with more limited resources. Additionally, the widely adopted standards such as ISO/IEC 27559:2022 or ISO/IEC 20889:2018 would be a good point of reference to support all companies in their compliance efforts. In addition, many companies from various sectors would benefit from practical tool boxes being added to the Guidelines allowing them to become more practical and useful[12]. Moreover, such additions would align the final Guidelines with the EDPB's Helsinki's commitment to provide concise guidance that is accessible, easy to understand, and practical for SMEs.

It would also be helpful for the final Guidelines to address PETs more substantively. Practical examples could explain how techniques such as differential privacy, secure multiparty computation, homomorphic encryption and synthetic data may contribute to anonymisation in appropriate circumstances, while recognising that their effectiveness must be assessed in the relevant context. Beyond practical guidance, the final Guidelines should also identify and

[12] It was also raised in the cross-industry letter requesting more practical EDPB guidance https://www.fedma.org/wp-content/uploads/2025/11/251117-Letter-to-EDPB-on-upcoming-stakeholder-event-on-anonymisation-and-pseudonymisation.pdf

reference existing standards and recognised frameworks for PETs that companies can rely on when selecting and implementing these technologies. It could be useful to draw on the relevant works of the Organisation for Economic Co-operation and Development[13] while doing so. This would provide businesses with greater legal certainty and practical benchmarks for assessing the effectiveness of PETs. Moreover, such guidance would better reflect the current state of the art and could encourage investment in solutions that make effective anonymisation, that is the ultimate PET, more accessible also to SMEs and start-ups.

Accordingly, the contextual approach should receive at least equal visual and substantive prominence in the main text. The simplified approach could be expressly described as an optional, conservative screening tool, accompanied by confirmation that no adverse inference should arise solely from an organisation's decision not to use it and that any enforcement finding must be based on a contextual application of art. 4(1) and recital 26 GDPR.

5) Mixed datasets

We recommend revising paragraph 36 of the draft Guidelines to distinguish more clearly between the obligations applicable to personal data within a mixed dataset and the legal status of the anonymous data it also contains. The analogy with CJEU C-252/21 *Bundeskartellamt* judgement is insufficient - paragraph 89 of this ruling concerns sensitive and non-sensitive personal data that cannot be separated at collection, rather than the status of anonymous information. A more proportionate and practicable approach would allow organisations, subject to accountability, to demonstrate which records remain anonymous through a documented, contextual assessment of whether the components can be reliably distinguished and whether identifiable records compromise the anonymity of the remainder. Re-identification of one individual, as indicated in paragraph 87 draft Guidelines, should trigger that assessment without automatically determining the status of unrelated records. The final guidelines should recognise appropriate technical and organisational controls and respect Recital 26's exclusion of anonymous information.

[13] https://www.oecd.org/en/topics/sub-issues/privacy-enhancing-technologies.html

6) Tension between the Digital Markets Act and the GDPR

The Alphabet decision[14] exposes a substantive divergence between the Commission's approach under art. 6(11) DMA and the approach reflected in the draft Guidelines. Under paragraphs 34 and 89-91 of the draft, technical, organisational and contractual safeguards may influence which means are reasonably likely to be used for re-identification, but they cannot by themselves render a dataset anonymous. In particular the draft Guidelines point out that encryption remains reversible and a contractual prohibition cannot be treated as equivalent to a prohibition imposed by law. In its final measures of 16 July 2026 in Case DMA.100209, however, the Commission appears to accord those safeguards materially greater weight - it characterises the search dataset as anonymised because technical alteration plays a "prominent role" and contractual, eligibility, monitoring and audit requirements reduce the residual risk of re-identification to an insignificant level. The resulting tension concerns not merely the sufficiency of contracts in isolation, but the legal significance attributed to a regulated combination of safeguards when identifying the means "reasonably likely to be used". The draft Guidelines may be read as requiring anonymity to arise principally from alteration of the data, with access and contractual controls serving only a supporting function, whereas the Commission's approach permits those controls particularly when imposed through a binding regulatory decision to contribute decisively to the conclusion that the data are anonymous for the authorised recipients. The final Guidelines should reconcile these positions expressly. They should preserve the distinction between a contractual undertaking and a prohibition by law while clarifying when a layered and enforceable framework such as combining data alteration, access restrictions, recipient eligibility, purpose and onward-sharing limitations, monitoring, audits, and effective remedies may make re-identification insignificant in practice. Without such clarification, the same safeguards may lead to opposing assessments under the GDPR and the DMA, undermining legal certainty and the consistent application of law. This divergence should be resolved either in the final EDPB Anonymisation Guidelines or in the final Guidelines Joint Guidelines on the interplay between the DMA and the GDPR. A clear explanation of any remaining difference would avoid conflicting regulatory standards and provide all organisations with the legal certainty needed to determine when shared data may reasonably be regarded as anonymous, regardless of whether they are subject to art. 6(11) of the DMA or other digital legislation, such as the Data Governance Act, the Data Act or the AI Act..

[14] See footnote 4.

7) Asymmetry among three criteria

The “No Record Isolation”, “No Linkage” and “No Inference” criteria provide useful technical tests for identifying possible pathways to identification of a data subject. It may nevertheless be helpful to clarify that they are analytical tools rather than additional statutory elements of anonymity, since the ultimate legal question remains whether the information relates to an identified or identifiable natural person under art. 4(1) GDPR, assessed in light of recital 26. We welcome the fact that paragraph 52 explains that failure to satisfy any one criterion does not necessarily mean that the data are personal and that further analysis may be required. In this context, the results table in paragraph 97 could be read as applying a somewhat stronger consequence to failure of the “No Inference”[15] criterion than to failure of the “No Record Isolation” or “No Linkage criteria”. Further explanation of this distinction would be welcome, particularly as paragraph 80 recognises that linkage may also constitute a form of inference, while paragraphs 67–71 and 87 indicate that the relevance of an inference depends on its specificity, meaningfulness, accuracy and capacity to enable an individual to be distinguished and treated differently. To promote clarity and consistent application, the EDPB should therefore align the results table in paragraph 97 more closely with paragraph 52 or provide the reasons for a different treatment regarding the “No Inference” criterion there. Failure of any criterion should lead to an appropriate further assessment of whether the information identifies, or renders identifiable a natural person.

The final Guidelines could also usefully clarify the consequences of successful identification of isolated records within a larger dataset. The identification of a single record should not automatically determine the status of an entire dataset. Instead, the relevant assessment should focus on whether the factors permitting identification of one record materially affect the identifiability of the remaining records.

8) Reassessment

It is true that anonymity may change over time due to technological developments, the evolving state of the art and relevant changes in the capabilities of the entities processing the data. However, because genuinely anonymous information falls outside the GDPR, the final

[15] When this criterion is violated, the table indicates that “the data **should not be** considered anonymous from at least one of the relevant perspective”, for the "No Record Isolation” and “No Linkage criteria” the conclusion is different when they fail - “the data **may not be** anonymous from one of the relevant perspective”. There is no explanation regarding this difference.

Guidelines should clarify the limits of the reassessment expectation and avoid implying a perpetual GDPR monitoring duty towards the data that was initially assessed as non-personal. In particular, they should identify whether reassessment is expected from the anonymising controller, the entity currently using the dataset or other actors as well. Including a concise, risk-based reassessment matrix setting out the responsible actors, core trigger events, proportionate review intervals and the consequences of a changed assessment. The documentation retained under paragraph 41 should record the assumptions underlying the original assessment, the agreed triggers for review and the allocation of responsibilities. Finally, the final Guidelines should clarify that reclassification operates prospectively. The original assessment should be judged against the information and technology available at the relevant time. If the likelihood of identification later ceases to be insignificant, the relevant entity should treat the data as personal from the point at which it knows, or reasonably ought to know, of that change. A subsequent change in circumstances should not, by itself, render earlier processing unlawful where the original assessment was reasonable and properly documented. Likewise, new data, technologies, or techniques should not automatically make an earlier assessment invalid if it was based on the best information and methods available at the time.

***

We thank you in advance for taking into consideration these concerns and suggestions to ensure that this public consultation leads to meaningful changes to the draft Anonymisation Guidelines.