SVENSKT NÄRINGSLIV

European Data Protection Board

2026-09-30

Comments

Regarding EDPB Guidelines 02/2026 on Anonymisation

Summary

The Confederation of Swedish Enterprise welcomes the European Data Protection Board's efforts to clarify anonymisation and promote consistent application of the General Data Protection Regulation (GDPR). We particularly welcome the recognition that identifiability must be assessed in context and from the perspective of the relevant entity. Information may be personal data for one entity while being anonymous for another, depending on the information and means of identification reasonably available in the circumstances. The assessment should be based on objective factors and focus on whether identification is reasonably likely in the relevant context, taking account of effective technical, organisational, contractual and legal safeguards.

The final Guidelines should provide greater legal certainty, address real processing situations and apply a proportionate, risk-based and innovation-friendly approach. They should explain not only why anonymisation fails, but also how it can be achieved. This requires clearer legal tests, balanced examples, recognition of effective safeguards, practical guidance for unstructured and visual data and stronger support for privacy-enhancing technologies.

To further improve the draft Guidelines the Confederation of Swedish Enterprise encourages the EDPB to

- simplify the assessment framework
- confirm that the contextual approach reflects the legal assessment under Recital 26 GDPR
- clarify No Record Isolation, No Linkage and No Inference
- distinguish realistic identification risks from remote possibilities
- recognise internal segregation and recipient-specific assessments
- clarify the position of processors
- improve terminology

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 (0)8 553 430 00
svensktnaringsliv.se Org. Nr: 802000-1858

- align the anonymisation and pseudonymisation Guidelines
- clarify the GDPR's material scope with respect to anonymous information
- provide positive examples of successful anonymisation
- address free text, call transcripts, images, video and AI systems
- revise example 8
- give appropriate weight to legal, contractual, technical and organisational safeguards
- support the development and adoption of PETs, including differential privacy
- take a proportionate approach to mixed datasets and outliers
- establish risk-based documentation requirements
- limit reassessment to material changes
- provide practical implementation tools and references to relevant technical standards.

1. Legal certainty and practical applicability

1.1 A clearer assessment framework

The proposed framework is unnecessarily complicated. The three criteria can be understood individually, but their combined application, their relationship with Recital 26 GDPR and the distinction between the simplified and contextual approaches are insufficiently explained. Annex 1 illustrates rather than resolves this difficulty and may lead organisations and supervisory authorities to different conclusions in comparable cases.

The final Guidelines should present the assessment as a coherent sequence of questions, explain the legal function and interaction of the three criteria and support the analysis with a concise checklist and complete worked examples. The objective should be to enable a reasoned and defensible conclusion, not merely identifying every factor that could conceivably be relevant.

1.2 The contextual approach and the likelihood standard

The final Guidelines should state expressly that the contextual approach reflects the legal assessment under Recital 26 GDPR. The relevant question is whether a person is identified or identifiable from the perspective of the entity concerned, taking account of the data, processing environment, access to additional information and safeguards. The simplified approach may be useful as an initial screen, but it should not become a separate or stricter legal standard or create a presumption that information is personal data.

The Guidelines correctly reject a zero-risk standard, but "means reasonably likely to be used" and "insignificant in reality" require greater precision. Factors increasing identifiability must be weighed against those reducing it, including practical access to auxiliary data, time, cost, expertise, computing resources, the probability of successful identification and effective technical, organisational, contractual and legal safeguards. The Guidelines should explain how these factors interact rather than simply list them.

1.3 No Inference, internal segregation and recipients
No Inference gives rise to particular uncertainty. The Guidelines should distinguish a specific and meaningful inference about an identifiable person that depends on the relevant dataset from a general conclusion based on population-level patterns, public information or general knowledge. Ordinary statistics, benchmarking and machine-learning generalisation should not prevent anonymity unless they reveal or enable a meaningful conclusion about an identifiable person based on that person's underlying data. Examples should address membership inference, model memorisation and extraction, as well as population-level analytics and generalised model outputs.
The contextual approach should also recognise technical and organisational separation within legal entities and corporate groups. A business unit should not be deemed to possess all information and capabilities available elsewhere in the organisation merely because an organisational connection exists. Role-based access controls, system separation, restrictions on recombination, monitoring and enforceable internal rules may materially affect identifiability.

The same applies to processors and other recipients. Information may be anonymous from a processor's perspective where the processor receives only a limited or transformed dataset, lacks access to identifying information and is prevented by binding instructions and technical measures from obtaining or using it. Automatically attributing the controller's means of identification to the processor would undermine the contextual approach and weaken incentives for data minimisation.

1.4 Terminology, pseudonymisation and the GDPR's scope
The final Guidelines should distinguish between "anonymous", "anonymised", "de-identified", "de-personalised" and "pseudonymised". They should prohibit misleading claims of anonymity without treating all terms for intermediate risk-reduction measures as legally equivalent.

The EDPB should also ensure consistency with its guidance on pseudonymisation. Although the concepts are legally distinct, both involve questions about additional information, relevant entities and technical and organisational separation. The two instruments should be finalised in a coordinated manner and should explain how the entity-relative anonymity assessment relates to the "pseudonymisation domain".

Finally, the Guidelines should be precise about the GDPR's material scope. Anonymous information does not automatically return within the GDPR merely because it is transferred, retained or used for another purpose. The decisive issue is whether the changed context gives the relevant entity means reasonably likely to be used for identification.

2. Concrete real-world use cases
2.1 Positive and complete examples
The draft focuses predominantly on circumstances in which anonymisation fails. Organisations also need examples showing how the threshold can be met. The final text should include complete analyses of aggregated commercial and market insights, controlled business-to-business sharing, segregated internal use, AI training and

evaluation, synthetic data, unstructured text, visual data and privacy-enhancing technologies. Each example should identify the relevant entity, data and realistic identification pathway, explain available auxiliary information and safeguards and, where useful, show which factual change would alter the result.

2.2 Unstructured data and layered retention

The current examples are largely tabular, although organisations frequently seek to anonymise correspondence, complaint records, notes and transcripts. The legal test should not vary with data format, but the Guidelines should explain how filtering, redaction, generalisation, summarisation and aggregation can be combined with contextual testing for unstructured data.

A dedicated example should address conversational text derived from recorded calls.[1] Call transcripts may retain direct or indirect identifiers, sensitive contextual details and operational metadata such as timestamps, ticket numbers and customer or employee references. The example should address the strengths and limitations of automated redaction, retained operational identifiers, AI-generated summaries and deletion of the source audio. A transcript that remains linkable through contextual information should continue to be treated as personal or pseudonymised data.

The Guidelines should also address different representations of the same information retained for different purposes and periods.[2] A source recording may be kept for evidentiary or regulatory reasons, while a redacted transcript or analytical output is retained separately for quality assurance, trend analysis or model validation. The original data's continued lawful retention should not automatically prevent a derivative from being anonymous for an entity that cannot realistically access and combine the data layers. The Guidelines should explain how segregation, deletion of source data, differing retention periods and reassessment affect the analysis.

2.3 Images, video and AI systems

A worked example is also needed for camera-derived images and video.[3]
The example should address facial blurring and pixelation, technical reversibility, reconstruction and enhancement, image quality, and residual identification through gait, clothing, surroundings, accompanying persons and metadata. The Guidelines should clarify when such measures merely reduce visibility and when they can reduce identification risk to an insignificant level, including where only some people in the footage are masked.

AI-specific examples should address training and evaluation data, synthetic data, model outputs, membership inference, memorisation and extraction. The Guidelines should

[1] This example reflects practical experience in call-center and alarm-monitoring operations. The underlying issues are also relevant to financial services, insurance, healthcare telephony, retail and other customer-service operations.
[2] This issue concerns, among other situations, source recordings retained for evidentiary or regulatory purposes and transcripts or derived outputs retained separately for quality assurance, analytics, training and process improvement.
[3] Blurring and pixelation are commonly used in camera-based security and alarm-verification contexts, but the draft Guidelines do not clarify whether those techniques can meet the anonymity threshold or should be treated only as mitigating measures.

distinguish population-level generalisation from information that reveals or depends on an identifiable person’s data and explain what evidence may support the conclusion that a model or output is anonymous.

3. Risk-based and innovation-friendly regulation

3.1 Realistic risks and effective safeguards

The GDPR does not require identification risk to be eliminated absolutely. Rogue employees, cybercriminals, intelligence services and other adversarial actors should be considered only where there is a realistic pathway both to obtaining the information and successfully identifying a person. The assessment should consider foreseeable access routes, capabilities, auxiliary information, vulnerabilities, previous comparable incidents, security controls and the probability of success. The mere existence of a technically capable actor is insufficient.

Example 8 should therefore be revised. It should distinguish the mere possibility of an intrusion from a documented weakness creating a realistic access pathway and should show how remedial measures can change the outcome. A paired counterfactual would demonstrate that the assessment responds to improved security rather than being predetermined by a hypothetical failure.

Contractual restrictions cannot alone make personal data anonymous, but neither should they be treated as cosmetic. Specific and enforceable prohibitions on re-identification, restrictions on onward disclosure, audit rights and meaningful remedies may, together with technical and organisational controls, materially reduce the likelihood of identification. Unlawful means should likewise be assessed proportionately. Organisations, especially SMEs, should not be required to speculate about criminal incentives or enforcement effectiveness across jurisdictions; the inquiry should focus on objective evidence of a realistic and foreseeable pathway to unlawful access and identification.

3.2 Future technology and privacy-enhancing technologies

Organisations should consider technological developments that are reasonably foreseeable, but they cannot be expected to predict unknown future capabilities. The abstract prospect of future AI advances should not prevent information from qualifying as anonymous today. The assessment should focus on demonstrated capabilities relevant to the data, their realistic accessibility and the time, cost, expertise and computing resources required.

The Guidelines should also give stronger support to privacy-enhancing technologies. They should explain how established and emerging techniques, including aggregation, generalisation, suppression, k-anonymity, differential privacy, secure multi-party computation, trusted execution environments, advanced cryptography, privacy-preserving synthetic data and federated approaches, may contribute to satisfying the three criteria. The guidance should remain non-exhaustive and technologically neutral and should explain strengths, limitations and common failure modes rather than create rigid safe harbours.

Differential privacy merits a worked example considering the selected privacy parameters, threat model, repeated releases, auxiliary information and implementation

quality. A theoretical residual risk should not by itself prevent a properly implemented technique from contributing materially to anonymisation.

3.3 Mixed datasets, documentation and reassessment
A small number of potentially identifiable outliers should not automatically determine the status of an entire large dataset. Organisations should be able to isolate, suppress or remove vulnerable observations, apply additional measures and reassess the residual dataset. Where the remaining likelihood of identification is insignificant in reality, the residual dataset should be capable of qualifying as anonymous. Genuinely anonymous information should not become personal data solely because it is stored alongside personal data.

Documentation should be proportionate to the data, processing scale, recipients, techniques, potential consequences and expected period of use. The EDPB should provide a short model assessment covering the relevant entities, realistic identification pathways, auxiliary information, safeguards, testing, conclusion and review triggers. Reassessment should be required following a material change, such as expanded access, a new recipient, a relevant auxiliary dataset, a security incident, a change in method or a demonstrated and realistically accessible identification capability. General technological development should not require every assessment to be reopened. Reviews should be integrated into existing GDPR accountability and security processes where appropriate.

A concise implementation annex should bring these elements together through a checklist, a model assessment, positive and negative examples and indicative reassessment triggers. References to recognised frameworks such as NISTIR 8053 and ISO/IEC 20889:2023 would be helpful, provided that compliance with a technical standard is not treated as determinative of the legal status of information under the GDPR.

Conclusion
The Confederation of Swedish Enterprise supports the EDPB’s objective of clarifying anonymisation and promoting consistency across the European Union. The recognition of a contextual and entity-relative assessment is an important foundation, but the final Guidelines must translate that principle into a clear, proportionate and operationally useful framework.

Anonymisation should not be assessed against every theoretically conceivable attack, unknown future technology or hypothetical act of non-compliance. The focus should be on whether identification is reasonably likely in the relevant context and on the combined effect of effective technical, organisational, legal and contractual safeguards.

A shorter and clearer framework, supported by positive real-world examples and proportionate rules for documentation, reassessment and mixed datasets, would improve legal certainty while preserving a high level of protection. It would also strengthen incentives to use privacy-enhancing technologies and enable responsible data use for research, inn Below is a fully revised version with improved structure, tighter legal reasoning and more consistent terminology. It retains the three-pillar

structure, integrates all identified company input, and distinguishes more clearly between the applicable legal test, operational guidance and policy recommendations.

SVENSKT NÄRINGSLIV

Carolina Brånby