EDPB Guidelines on anonymisation

Executive summary

FEDMA welcomes the publication of the draft guidelines on anonymisation, particularly because effective anonymisation is essential to protecting individuals while enabling the lawful and responsible use of information for research, innovation, statistical analysis, competition and economic activity. A clear and workable framework for anonymisation can strengthen legal certainty and support privacy-preserving innovation in Europe, enabling European businesses to develop competitive data-driven products and services.[1] The GDPR is not intended to prohibit data use as such. It establishes a framework for the protection of individuals and the lawful processing and free movement of personal data within the Union. Once information is anonymous under the applicable legal standard, its use should not be unnecessarily constrained by requirements intended for personal data.

FEDMA supports the EDPB's objective of clarifying the concept of anonymity, including the need to address risks of re-identification. However, the final Guidelines must fully reflect Article 4(1) and Recital 26 GDPR, the CJEU's case law and the respective roles of legal definitions and technical assessment methodologies.

In particular, FEDMA recommends that the EDPB:

1. **Preserves a contextual, risk-based and evidence-based approach to identifiability.** The assessment must distinguish technical possibility from means reasonably likely to be used, taking account of the relevant entity, realistic access to additional information, applicable safeguards, costs, technological capabilities and actual identification risks. The possibility that information may become identifiable in different circumstances or at a later stage should not, in itself, prevent it from being considered anonymous for the relevant entity under the circumstances prevailing at the time of the assessment.
2. **Ensures that technical criteria do not become additional legal conditions.** No Record Isolation, No Linkage and No Inference are important assessment tools, but their interpretation and practical application must remain consistent with the legal definition of personal data. Voluntary or precautionary methodologies should not become de facto mandatory standards.

[1] Mario Draghi, The Future of European Competitiveness – Part A: A Competitiveness Strategy for Europe, 9 September 2024, particularly p. 79 and 319. https://commission.europa.eu/topics/competitiveness/draghi-report_en.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

3. **Recognises anonymisation as a privacy-enhancing activity.** The Guidelines should provide clearer guidance on the applicable legal bases for anonymisation, including where it supports compliance with GDPR obligations or forms part of a legitimate processing activity designed to produce anonymous outputs.
4. **Ensures coherence with the wider EU legal framework.** Data protection must be interpreted consistently with the Charter of Fundamental Rights, the GDPR's objectives, EU treaties, the free movement of non-personal data, competition and the legitimate development of privacy-preserving technologies. The Guidelines should also support the responsible data-sharing objectives of the European strategy for data and Common European Data Spaces by providing legal certainty for the production and use of anonymous information, without altering the applicable legal standard of anonymity.
5. **Provides operationally effective guidance.** Proportionate threat models, objective evidentiary criteria, differentiated examples and sector-specific implementation tools would reduce legal uncertainty and support consistent application across Member States, particularly for SMEs and new market entrants.

The right to data protection is fundamental, but it is not absolute. As Recital 4 GDPR expressly recognises, it must be balanced with other fundamental rights in accordance with the principle of proportionality. Neither privacy protection nor other fundamental rights or other compelling interests should be treated as automatically prevailing in every situation independently of the applicable legal framework.

FEDMA therefore calls for final Guidelines that provide robust protection against genuine identification risks while enabling the effective development and use of anonymous data. Such an approach would strengthen individuals' rights, legal certainty, innovation and European competitiveness.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Contents & overview of positions

1. General observations 6
The Guidelines should be better aligned with existing stakeholder input, policy objectives and regulatory frameworks 6
The EDPB must support operational compliance through industry collaboration and sector-specific implementation tools 9
2. Legal analysis **10**
a. Whether the information relates to a natural person **13**
The distinction between personal data and aggregated data should be preserved ... 13
The "effect" part of the "relates to a person" assessment should focus on concrete and objectively foreseeable consequences of processing 15
b. Whether the natural person is "identified" or "identifiable" **15**
The concept of identifiability should remain distinct from the "relates to a person" assessment 15
When assessing identifiability, the focus should be on "likely" (not "possible") identification 16
Singling out should not automatically be equated with identification 18
The "means reasonably likely to be used" assessment should embed the relative approach (i.e. identifiability should be assessed from the perspective of the relevant entity) 18
The "means reasonably likely to be used" assessment should fall back on realistic capacities rather than speculative occurrences 19
c. Additional considerations (mixed datasets and anonymisation as a data processing activity) **22**
Personal and non-personal data should not automatically be treated alike 22
The Guidelines should not include unnecessary barriers to effective anonymisation 23
3. Technical analysis **25**
The technical assessment should support, rather than replace, the GDPR legal test for anonymisation 25
The distinction between technical evidence and legal classification should be reflected in every adverse conclusion arising from the three criteria. 27
a. The three criteria **27**

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

The three criteria should be complementary technical tests, not cumulative legal requirements 27

Provide a proportionate and documented assessment framework, rather than mandatory thresholds or certification 28

Technical evidence should be assessed contextually and according to the nature, reliability and operational relevance of the technique concerned 28

b. No Record Isolation 29

Record uniqueness should be an indicator, not proof of identifiability 29

The Guidelines should also avoid treating a single minimum group size or a particular k-anonymity configuration as a universal legal condition 29

c. No Linkage 30

There should be a consistent distinction between technical linkability, reliable matching of records relating to the same person, and the identification or identifiability of that person. 30

Linkage should be assessed by reference to the relevant actor's realistic ability to access and use the additional information, rather than the mere existence of technical linkability with another dataset. 30

Actual access conditions, contractual restrictions, technical segregation and other effective safeguards should be considered when determining whether linkage is reasonably likely 31

d. No Inference 31

The ability to derive general statistical or predictive information should be distinguished from a demonstrated specific and meaningful inference concerning an individual 31

The Guidelines should distinguish between different inference techniques and require their actual capacity to produce a specific and meaningful individual-level inference to be demonstrated 32

A specific inference should not presuppose the identification or identifiability it seeks to establish 33

A counterfactual test should not require organisations to retain, reconstruct or reacquire identifiable source data where another technically reliable method can establish the relevant facts 33

A failure of No Inference should not automatically determine the legal status of the data without demonstrating a specific and meaningful individual disclosure 34

4. The interplay between the legal and technical analysis 35

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Technical findings should inform, but not replace, the legal assessment of whether information relates to an identified or identifiable natural person 35

Organisations should be free to apply the contextual approach directly, without first applying or failing the simplified approach 36

Compliance should be demonstrable through different scientifically sound and contextually appropriate methods, rather than a single prescribed methodology or technical threshold 37

5. Societal, economic and competition implications **38**

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

1. General observations

The Guidelines should be better aligned with existing stakeholder input, policy objectives and regulatory frameworks

While the draft Guidelines provide a detailed framework on anonymisation, they would benefit from stronger alignment with previous stakeholder contributions[2] and broader policy commitments. For instance, the Guidelines make limited reference to the input received during the EDPB stakeholder workshop on anonymisation and its report [3]. That report expressly records concerns raised by stakeholders regarding the contextual assessment of identifiability, the reasonable foreseeability of onward transfers, the practical limitations of assessing third parties' identification capabilities, the effectiveness of technical, organisational and contractual safeguards, and the role of privacy-enhancing technologies (PETs). These concerns deserve a clear and operational response in the Guidelines. The draft also does not sufficiently reflect the objectives set out in the EDPB Helsinki Statement,[4] notably the commitment to promote legal clarity, support innovation and strengthen engagement with stakeholders. In particular, greater attention should be given to the proportionality and practical feasibility of the proposed methodology, including its application by SMEs and new market entrants.

The Guidelines would also be strengthened by a more explicit explanation of how anonymisation interacts with other legislative instruments of the EU digital regulatory framework,[5] as well as by greater engagement with relevant international standards,[6] and guidance issued by other authorities[7]. This is particularly relevant where Union legislation expressly relies on anonymisation to achieve other regulatory objectives. For example, Article 6(11) of the Digital Markets Act requires the anonymisation of personal data included in certain search datasets made available to competing search engines, while Recital 61 recognises the importance of preserving the quality and usefulness of such data. Article 6(8) also establishes mechanisms for independent advertising verification, subject to applicable data protection requirements. The interpretation of anonymisation should preserve the practical effectiveness of these legislative provisions

[2] Cross-Industry Joint letter calling for practical EDPB guidance following the SRB ruling, 19th of November 2025 (weblink).

[3] Report on stakeholder event on anonymisation and pseudonymisation of 12 December 2025, 18th of February 2026 (weblink)

[4] The Helsinki Statement on enhanced clarity, support and engagement, 3rd of July 2025 (weblink).

[5] E.g. the Digital Markets Act (weblink), Digital Governance Act (weblink), Data Act (weblink), and the AI Act (weblink).

[6] E.g. ISO/IEC 20889:2018 on Privacy enhancing data de-identification terminology and classification of techniques and ISO/IEC 27559:2022 on Privacy enhancing data de-identification framework.

[7] E.g. the UK ICO guidance on anonymisation (weblink), the Office of the Information and Privacy Commissioner of Ontario's "De-identification Guidelines for Structured Data" (weblink) and the Personal Data Protection Commission of Singapore's "Guide to Basic Anonymisation" (weblink).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

without compromising the protection of individuals. The Guidelines should also integrate more operational, evidence-based and technologically neutral assessment methodologies, drawing, where appropriate, on established international standards and comparative approaches, such as the UK ICO's guidance on assessing the effectiveness of anonymisation.[8] This would also be consistent with the concerns identified in the Draghi Report regarding regulatory fragmentation, barriers to innovation and disproportionate compliance burdens on smaller businesses[9]. Such explanations would enhance legal certainty and regulatory coherence, facilitate proportionate implementation across Member States and provide greater predictability for undertakings seeking to apply anonymisation techniques in practice.

The Guidelines should also take account of the Union's broader objectives under the European strategy for data. The Commission's 2020 Communication envisages a single market in which data can flow across Member States and sectors, while fully respecting European rules on personal data protection, consumer protection and competition.[10] This ambition is being pursued through Common European Data Spaces in areas such as health, energy, mobility, agriculture, manufacturing and public administration, combining infrastructure and governance arrangements to facilitate trustworthy access to, sharing and reuse of personal and non-personal data.[11] The Commission expressly links greater data availability and use to innovation, competitiveness and societal benefits, including better healthcare, more sustainable transport and more efficient public services.[12]

Effective anonymisation can contribute to these objectives by enabling the production and use of genuinely anonymous information. FEDMA therefore considers that clear, proportionate and technologically neutral guidance on anonymisation is important to the practical implementation of the Union's data strategy. The Guidelines should preserve the distinction between the lawful processing and sharing of personal data subject to the GDPR and the use of information that is anonymous under the standard established by Article 4(1) and Recital 26. These policy objectives do not alter that legal standard, but

[8] The UK ICO guidance on anonymisation (weblink).
[9] Mario Draghi, The Future of European Competitiveness – Part A: A Competitiveness Strategy for Europe, 9 September 2024, particularly pp. 29–30 and 68–69. https://commission.europa.eu/topics/competitiveness/draghi-report_en.
[10] European Commission, A European strategy for data, COM(2020) 66 final, 19 February 2020, Section 3, (weblink); see also European Commission, "Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence", press release IP/20/273, 19 February 2020, section "Europe as a leader in the data economy" (weblink).
[11] European Commission, "Common European Data Spaces", Shaping Europe's digital future, updated 14 August 2026, sections "Building the single market for data" and "Concept" (weblink).
[12] European Commission, "A European strategy for data", Shaping Europe's digital future, updated 20 August 2026, (weblink); see also COM(2020) 66 final, Section 1 (weblink).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

they reinforce the importance of avoiding unnecessary uncertainty or additional substantive conditions that could impede effective anonymisation and useful data sharing without a corresponding improvement in the protection of individuals.

The Guidelines would, in particular, benefit from explaining more clearly the relationship between anonymisation and other established concepts, such as pseudonymisation, de-identification, non-personal data, synthetic data and privacy-enhancing technologies. Building on the recognition in paragraph 39 that immediate anonymisation can reduce the impact of processing on data subjects, the Guidelines should further explain how effective anonymisation operates as a privacy-enhancing process supporting data minimisation and data protection by design and by default under Article 25 GDPR. Its protective function should be expressly reflected when assessing the effectiveness and proportionality of anonymisation measures. To promote legal certainty and coherence across the EU digital regulatory framework, FEDMA recommends expanding and refining the existing glossary in Section 4 of the Guidelines, so that it clearly distinguishes established legal definitions from technical concepts and explains the relationship between anonymisation, pseudonymisation, de-identification, synthetic data, non-personal data and PETs. The glossary should refer to established concepts in EU law and relevant technical standards, without creating parallel definitions or additional substantive legal requirements. It should also distinguish technical measures that mitigate identification risks from the legal determination that information is anonymous, without introducing additional substantive requirements beyond Article 4(1) and Recital 26 GDPR. The use of a particular PET should neither automatically establish nor automatically preclude a finding of effective anonymisation. Providing a common terminology framework would help undertakings, national data protection authorities (as well as other relevant authorities) and other stakeholders better understand the legal and practical distinctions between these concepts and how they relate to anonymisation.

More generally, the Guidelines should reflect that data protection law does not merely provide mechanisms for individual control over personal data. It establishes the conditions under which personal data may be processed lawfully, fairly, transparently and responsibly, while protecting the rights and freedoms of individuals. Effective anonymisation advances these objectives by reducing the need for identification and enabling the generation of useful information without unnecessarily exposing individuals to identifiable data. The EDPB should therefore promote interpretations and technical methodologies that support, rather than inadvertently discourage, effective anonymisation as a means of responsible data governance.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

The EDPB must support operational compliance through industry collaboration and sector-specific implementation tools

The Guidelines provide a comprehensive theoretical legal and technical analysis, but their practical application will inevitably vary across sectors, business models and use cases. While ensuring a uniform interpretation of Article 4(1) and Recital 26 GDPR, the EDPB should actively encourage and support the development of sector-specific implementation tools, including codes of conduct under Article 40 GDPR, industry best practices and operational checklists, as well as proportionate risk-assessment templates, evidence-based threat models and practical implementation examples. Such tools should be developed through structured cooperation between industry associations and supervisory authorities, reflecting the actual characteristics of different processing operations, recipients, technologies and access conditions. They should facilitate compliance without treating optional methodologies or case-specific technical parameters as generally mandatory conditions of anonymity, while preserving the existing powers of supervisory authorities and promoting consistent application across Member States. This would help undertakings, particularly SMEs (often lacking dedicated in-house privacy expertise), translate the Guidelines into effective compliance measures while taking account of the specific characteristics and risks of different sectors. It could also reduce unnecessary compliance costs for startups and new market entrants, while supporting consistent application across the internal market.

Sector-specific examples could benefit from a more nuanced and sector-neutral approach. For instance, footnote 27 refers to information about a person's hobby being economically valuable for targeted marketing purposes. While FEDMA welcomes the clarification that the potential value of data should be distinguished from its sensitivity, the specific reference to targeted marketing could unintentionally create the impression that this sector has a particular incentive to re-identify anonymised data. However, the commercial value of information should not be confused with the technical capability or reasonable likelihood of identifying an individual. Economic incentives may constitute a relevant factor in the assessment, but cannot, in isolation, establish that re-identification is reasonably likely to occur. In practice, significant economic value can be generated through marketing and advertising practices that do not require the identification or re-identification of individual consumers, such as through anonymised aggregate campaign reporting and privacy-preserving audience measurement. Moreover, the potential value of re-identified data arises across a wide range of sectors. Any assessment of re-identification incentives should therefore remain grounded in objective evidence concerning the relevant actor's actual capabilities, access to additional information, costs, practical obstacles and reasonably foreseeable conduct, rather than assumptions derived from the commercial purpose of the processing. The

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Guidelines would therefore benefit from either using more sector-neutral examples or illustrating how the concept of value differs across sectors, while leaving more granular and sector-specific appreciations to industry-led initiatives.

Moreover, the examples in the Guidelines should also reflect a broader range of processing environments, sectors and levels of re-identification risk. In particular, FEDMA encourages the EDPB to include differentiated examples involving statistical reporting, surveys, direct marketing, audience measurement, market research, B2B company-level analytics and research outputs, alongside more demanding cases involving detailed location information, persistent online identifiers or rare and sensitive attributes. This would better reflect the diversity of the European data and marketing ecosystem, which extends beyond online behavioural advertising. Such examples should make clear that the same legal standard applies throughout the EU, while recognising that proportionate technical assessments and effective safeguards may differ depending on the processing environment.

Building on the balanced approach taken in earlier Article 29 Working Party guidance, the Guidelines should also provide a more balanced set of practical examples illustrating both when anonymisation is successful and when it is not. For example, FEDMA recommends examples of successful and unsuccessful record linkage, including cases where two datasets can be matched with high probability but no relevant actor can reasonably identify a natural person, as well as cases where a nominally aggregated output can be joined with accessible auxiliary information to reveal an individual. This would improve the operational value of examples 11-12 and 25 while respecting the qualifications in paragraphs 61, 64-65 and 101-103.

2. Legal analysis

The legal analysis in the Guidelines is understood and summarised as follows:

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

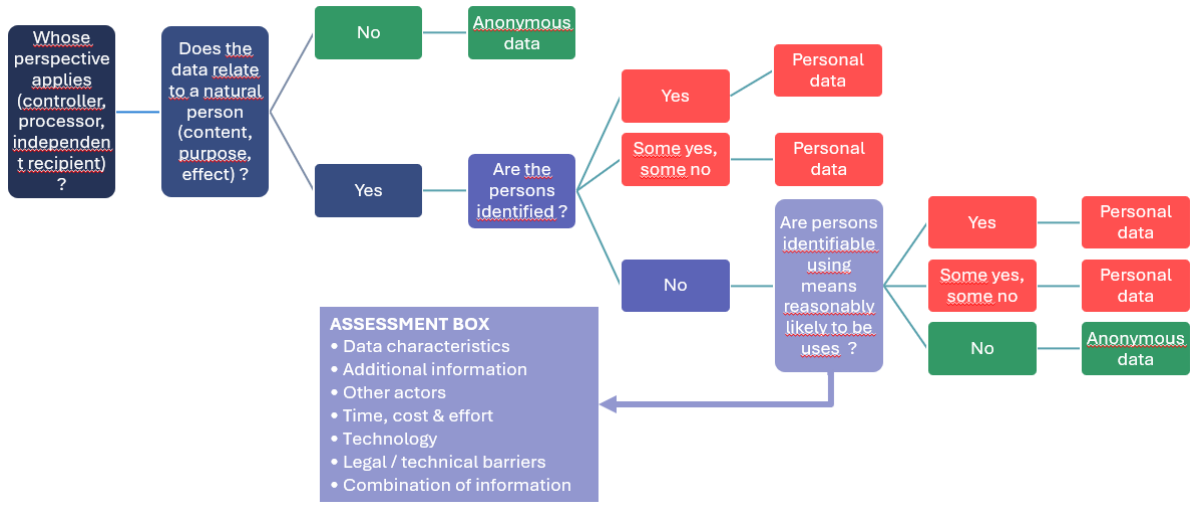


Figure 1: Illustrative representation of the legal assessment under Article 4(1) and Recital 26 GDPR. The assessment remains contextual and depends on the relevant perspective, processing circumstances and means reasonably likely to be used for identification.

As a general remark, the legal basis of the Guidelines is Article 70(1)(e) GDPR, and the core objective of this mandate is to promote the consistent application of the GDPR. The EDPB can therefore clarify the interpretation and application of the GDPR, including in light of the principles established by the CJEU, within the limits of the existing legislative framework. This requires maintaining a clear distinction between interpreting the legal criteria established by Article 4(1) and Recital 26 GDPR and introducing additional substantive conditions for recognising information as anonymous. **The EDPB's interpretative mandate must also be exercised consistently with the principle of conferral under Article 5(1) and (2) TEU and the institutional framework established by Union law. Article 70(1)(e) GDPR empowers the EDPB to promote consistent application of the Regulation through guidelines, recommendations and best practices; it does not confer an independent legislative competence to modify the conditions under which information constitutes personal data[13]. Accordingly, the Guidelines should expressly distinguish legally binding requirements established by Union law from recommended technical methods, evidentiary indicators and precautionary practices. Neither the presentation of a methodology as authoritative nor its subsequent use in supervisory practice should obscure that distinction**. However, certain parts of the draft do not yet translate the applicable legal standard into sufficiently clear and operational guidance, particularly regarding the assessment of means reasonably likely to be used for identification, the relevance of third-party identification capabilities, and the evidentiary weight of technical, organisational and

[13] Article 5(1)–(2) TEU; Article 70(1)(e) GDPR.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

contractual safeguards. These issues require further clarification to ensure that the same legal standard can be applied in a predictable, realistic, evidence-based and consistent manner across the Union.

Furthermore, the EDPB should take full account of Article 1(1)-(3) GDPR, which combines the protection of the fundamental rights and freedoms of natural persons with rules governing the free movement of personal data within the Union. The EDPB Guidelines on anonymisation should therefore ensure that the scope of the GDPR remains determined by the legal criteria of Article 4(1) and Recital 26, rather than by precautionary presumptions extending beyond the applicable standard of identifiability. Where the draft Guidelines introduce uncertainty or unnecessary obstacles to the effective use of anonymisation, they risk discouraging the lawful transformation of identifiable data into anonymous data and unnecessarily restricting the legitimate use and cross-border exchange of such information, without a demonstrated corresponding improvement in the protection of data subjects. This is particularly relevant where effective anonymisation contributes to data minimisation, reduces exposure to identifiable information and supports privacy-preserving innovation. The processing of personal data during anonymisation must, in any event, remain subject to the applicable GDPR requirements.

This interpretation must also reflect the constitutional framework of the Union. Article 8 of the Charter guarantees the fundamental right to the protection of personal data[14], while Article 16 protects the freedom to conduct a business. Recital 4 GDPR expressly recognises that the right to data protection is not absolute and must be balanced against other fundamental rights in accordance with the principle of proportionality.

Accordingly, data protection should not be treated as automatically overriding the freedom to conduct a business or other protected interests irrespective of the applicable legal framework and the circumstances of the case. Equally, economic interests cannot justify the disregard of data protection obligations or diminish the protection guaranteed by the GDPR. The proper approach is to give effect to the requirements and balancing mechanisms established by Union law, including the conditions for lawful processing and the legal distinction between personal and anonymous data.

Where an interpretation of anonymity creates additional practical restrictions on the lawful use of information, the EDPB should be able to explain how those restrictions follow from the GDPR's legal definition and why the resulting requirements are necessary and proportionate to the identification risks concerned. This is particularly important

[14] Charter of Fundamental Rights of the European Union, Articles 7, 8, 16 and 52(1); GDPR, Recitals 2 and 4 and Article 1.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

where less burdensome, technically demonstrable alternatives may provide equivalent or stronger protection for individuals.

FEDMA also encourages the EDPB to provide greater transparency regarding the objective factors, evidentiary requirements and limitations of the methodologies that organisations and supervisory authorities may use when assessing identifiability in practice. In particular, the Guidelines should clarify that the simplified assessment approach remains voluntary, that failure to satisfy an individual technical criterion does not automatically establish that information constitutes personal data, and that a properly substantiated contextual assessment should not be rejected merely because it does not follow a preferred technical methodology. Such clarification would help align assessments across Member States, strengthen legal certainty, and support a more consistent application of the GDPR.

a. Whether the information relates to a natural person

The distinction between personal data and aggregated data should be preserved

FEDMA welcomes the recognition that data can relate to an individual even where the link is not "readily apparent". However, paragraph 17 of the Guidelines recognises that aggregate information may relate to individuals where additional processing techniques could reveal an individual connection. While this correctly identifies a genuine risk in certain circumstances, the mere technical possibility of deriving individual-level information should not, in itself, determine the legal status of the original aggregate information. The mere fact that a dataset originates from personal data, or that further technical steps could derive from it data on an individual, does not automatically establish that the resulting information itself constitutes personal data.[15] The assessment should instead focus on whether the information relates to a natural person by reason of its content, purpose or effect and, separately, whether that person is identified or identifiable by means reasonably likely to be used, taking account of the relevant circumstances, available additional information and practical capabilities of the actors concerned. This distinction is already recognised in paragraph 18 of the Guidelines and should be consistently applied to the scenarios described in paragraph 17.

[15] See Joined Cases C-141/12 and C-372/12, YS and Others, judgment of 17 July 2014, paragraphs 38–40 and 48, where the CJEU distinguished personal data contained in an administrative document from the legal analysis based on those data. Although the case did not concern anonymisation or aggregated datasets, it illustrates that the use of personal data in producing information does not automatically determine the legal nature of every resulting element.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

This clarification is particularly important in the context of aggregated information. Data concerning groups, populations, trends or statistical outcomes should not be regarded as relating to specific persons solely because they originate from individual-level records. For example, aggregate conversion rates, audience statistics or demographic indicators may describe group-level behaviour, trends or characteristics without themselves relating to an identifiable individual. This does not exclude the possibility that sufficiently granular aggregates, small groups or particular combinations of attributes may allow information concerning individuals to be disclosed. Such risks must, however, be established through a contextual assessment of the information and the means reasonably likely to be used. Otherwise, many forms of aggregate data, metrics and analytical outputs and other types of enriched data could be treated as personal data merely because an individual inference is theoretically conceivable, even where the information reflects collective characteristics and no individual is reasonably identifiable in the relevant circumstances.

Marketing example
To describe a group, such as a particular neighbourhood, in aggregated form, the group's average value is often calculated. Examples are average age, average persons in a household and average probability of owning a car for a particular neighbourhood or street section, with a minimum of 4 households. Mathematically, this means adding up the values of all individual records and dividing the total by the number of households in that street section. Aggregation, as used for understanding neighbourhood characteristics, is therefore a many-to-one mapping: everyone in the group is assigned the same value. In addition, aggregation means the data no longer describes an individual, but instead reflects characteristics of a neighbourhood, making it non-personal data.

Importantly, paragraph 69 of the Guidelines expressly acknowledges that personal information may be inferred from data which are not themselves personal. Paragraphs 69–71 further distinguish general population-level inferences from specific and meaningful inferences connected to an individual. FEDMA recommends that paragraph 17 expressly reflect this distinction and clarify that the possibility of generating an

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

inference does not, without further assessment, determine the personal nature of the originating information[16].

The "effect" part of the "relates to a person" assessment should focus on concrete and objectively foreseeable consequences of processing

FEDMA welcomes the clarification in paragraph 16(c) that "there should be a *concrete possibility* that the individual can be treated differently from other persons as a result of processing of information". However, the Guidelines would benefit from clarifying that the effect element should be assessed by reference to the actual circumstances of the processing and its concrete, objectively foreseeable effects on an individual's rights or interests, including effects that may not have been intended but are nevertheless reasonably foreseeable. This would ensure that speculative scenarios are insufficient to establish that data relates to a person. In particular, the mere possibility that information may influence future decisions, or that aggregate information may affect a group or population, should not automatically establish that the information relates to a particular individual by reason of its effect. The assessment should identify a sufficiently concrete connection between the processing and the individual concerned, without dispensing with the separate requirement of identification or identifiability under Article 4(1) and Recital 26 GDPR.

b. Whether the natural person is "identified" or "identifiable"

The concept of identifiability should remain distinct from the "relates to a person" assessment

FEDMA welcomes the clarification that identification *involves* distinguishing an individual from others within a given context. However, paragraphs 19 and 25 link identification to the possibility of treating an individual differently. While distinguishing an individual may constitute identification in appropriate circumstances, the relationship between identification and differential treatment should not obscure the distinction between the two elements of the definition of personal data under Article 4(1) GDPR. To preserve that distinction, the Guidelines should clearly stipulate that the ability to affect, evaluate or differentiate between individuals may be relevant to the assessment of whether information relates to a natural person by reason of its purpose or effect, but does not dispense with a separate assessment of whether that person is identified or identifiable. The Guidelines would also benefit from clarifying that the

[16] EDPB, Guidelines 02/2026 on Anonymisation, paragraphs 18 and 69–71. See also CJEU, Nowak, C-434/16, paragraph 35, and EDPS v SRB, C-413/23 P, paragraphs 52–55 and 69–89, concerning the interpretation of information relating to an identified or identifiable natural person.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

possibility of treating individuals differently does not, by itself, determine whether they are identified or identifiable. In particular, the distinction between a natural person and a technical or statistical unit, such as a device, browser, session or record, should be assessed contextually, without assuming that the ability to distinguish the latter invariably establishes the identification of the former.

This distinction is particularly important in relation to the fourth example in paragraph 50, which refers to information used for evaluating, treating or influencing the status or behaviour of a specific individual. Unlike the preceding examples, which expressly refer to identifying attributes or means of identification, this example is framed primarily by reference to the purpose or effect of processing. While an individualised intervention may itself provide strong evidence of identifiability, the purpose of influencing a person cannot, as an independent proposition, replace the requirement that the natural person be identified or identifiable. The Guidelines should therefore distinguish individual-level targeting or recognition from aggregate statistical analysis and group-level outputs that may influence individuals without necessarily making the persons represented in the underlying information identifiable.

The EDPB may interpret and operationalise Article 4(1) GDPR; it cannot use guidance to replace the legislative requirement of an "identified or identifiable" natural person with a different legal threshold based solely on the purpose or effects of processing. Such an interpretation would risk altering the substantive scope of the GDPR, rather than clarifying it. FEDMA therefore recommends that paragraph 50 expressly confirm that the examples of immediately apparent personal data must satisfy both elements of Article 4(1), consistently with Recital 26, the CJEU's case law and the limits of the EDPB's mandate under Article 70(1)(e) GDPR[17].

When assessing identifiability, the focus should be on "likely" (not "possible") identification

FEDMA supports the Guidelines' recognition that anonymisation does not require the exclusion of all residual risks when assessing identifiability (paragraph 22). At the same time, paragraphs 20-21 emphasise that data subjects may remain identifiable where means of identification[18] *could* exist. Although these paragraphs refer to means reasonably likely to be used, greater clarification is needed regarding the objective circumstances in which potential access to additional information, cooperation between entities or subsequent transfers become relevant to identifiability. The

[17] GDPR, Articles 4(1) and 70(1)(e) and Recital 26; Article 16(2) TFEU; CJEU, Nowak, C-434/16, judgment of 20 December 2017, paragraphs 34–35.

[18] Such means may include obtaining additional information, applying identification techniques controlled by other parties or making information available to entities possessing means reasonably likely to be used for identification. See EDPB Guidelines 02/2026, paragraphs 20–21.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Guidelines should instead place greater emphasis on the *likelihood* of the means of identification being used, assessed in their practical context and in light of the likelihood of successful identification, rather than on purely theoretical possibilities. In particular, the assessment should distinguish a technically conceivable means, a legally available means, a means realistically accessible to a relevant actor, and a means reasonably likely to be used for identification. This is also consistent with the GDPR's risk-based approach, under which the nature and extent of appropriate measures should reflect the actual risks arising in the circumstances rather than seek to eliminate every conceivable risk irrespective of its likelihood. For the purposes of determining anonymity, the relevant assessment remains whether identification is reasonably likely through the means available in the circumstances, in accordance with Article 4(1) and Recital 26. A low expected impact on individuals does not, by itself, establish anonymity, just as a purely theoretical possibility of identification does not, by itself, preclude it[19].

As currently drafted, the combined application of certain provisions of the Guidelines may create the impression that any conceivable route to identification is sufficient to prevent a dataset from being considered anonymous. This impression would:

- risk divergent interpretations across Member States;
- undermine legal certainty;
- disincentivise the development and use of privacy-enhancing technologies and innovations that strengthen the protection of personal data; and
- encourage unnecessarily conservative compliance practices and disproportionate assessment costs, without a demonstrated corresponding improvement in the protection of data subjects.

Such consequences would be particularly relevant to SMEs, independent marketing service providers, publishers and innovative data analytics businesses that rely on proportionate and reproducible anonymisation assessments.

Moreover, such an outcome would be difficult to reconcile with the EDPB's commitment to promoting practical, risk-based guidance, facilitating GDPR compliance, and empowering responsible innovation[20]. FEDMA therefore recommends that the Guidelines provide clearer criteria for excluding remote or speculative identification scenarios, consistently with paragraph 22 and Recital 26 GDPR.

[19] Regulation (EU) 2016/679, Article 4(1), Recitals 26 and 75-76, and Articles 24(1) and 32(1); CJEU, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, judgment of 19 October 2016, ECLI:EU:C:2016:779, paragraphs 43-49, particularly paragraph 46.
[20] The Helsinki Statement on enhanced clarity, support and engagement, 3rd of July 2025 (weblink).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

This approach would also be supported by recent legal scholarship drawing together the CJEU's case law on anonymity. In his article, Roßnagel (Hessian Commissioner for Data Protection and Freedom of Information) observes that anonymity does not require the absolute exclusion of any possibility of identification. Rather, the assessment should focus on whether, in the specific circumstances, the relevant controller can realistically mobilise means that are reasonably likely to be used to identify the individual. A merely abstract or theoretical possibility of identification is therefore insufficient where the risk of identification is, in practice, *de facto* negligible.[21]

Singling out should not automatically be equated with identification

FEDMA welcomes the recognition that distinguishing a natural person from others within a given context may constitute identification, even where that person's civil identity is unknown. However, paragraph 25 and example 6 create the impression that the ability to single out a device, browser or technical identifier may, in itself, be sufficient to conclude that the corresponding natural person is identifiable. The Guidelines would benefit from clarifying that singling out must be assessed in relation to the natural person concerned and the actual capacity to distinguish that person within the relevant context. The fact that an entity can distinguish one record, device, browser or session from another does not necessarily mean that the corresponding person is identified or identifiable within the meaning of the GDPR. Identifiability should remain subject to a separate contextual assessment based on the means reasonably likely to be used and the realistic likelihood of linking the information to a person. FEDMA therefore recommends that the Guidelines distinguish technical uniqueness, persistent individual recognition and the identification of a natural person, supported by examples illustrating when these concepts overlap and when they do not.

The "means reasonably likely to be used" assessment should embed the relative approach (i.e. identifiability should be assessed from the perspective of the relevant entity)

The Guidelines place significant emphasis on the existence of additional information and potential chains of identification (paragraphs 28, 29(c)). However, well established CJEU case law confirms that the existence of additional information does not, in itself, imply that data are personal data for every entity.[22] FEDMA recommends that this principle be reflected more explicitly throughout the section on the "means reasonably likely to be used" assessment. In particular, the assessment should identify the relevant entity,

[21] Professor Dr Alexander Roßnagel, Anonyme Datenverarbeitung: Dogmatische Schlussfolgerungen aus der Rechtsprechung des EuGH, 2026.
[22] EDPS v SRB, C-413/23 P, judgment of 4 September 2025, paragraphs 75–89 and 99–115; OC v Commission, C-479/22 P, judgment of 7 March 2024, paragraphs 51–64; and Breyer, C-582/14, judgment of 19 October 2016, paragraphs 43–49.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

processing operation, applicable legal obligation and actual means of identification available to that entity, including any means that it is reasonably likely to obtain or use through other parties.

The Guidelines should also distinguish situations involving independent recipients from those involving processors acting on behalf of controllers. In this regard, paragraph 15 would benefit from further clarification of how the controller's perspective applies to processors, particularly where the processor has no independent means of identifying the individuals concerned. This should preserve the GDPR obligations applicable to processing carried out on behalf of a controller, while ensuring that obligations whose practical performance presupposes identification are interpreted in light of the processor's actual role, access and capabilities.

Furthermore, the possibility of an onward transfer should not lead to the automatic attribution of every hypothetical recipient's identification capabilities to all preceding entities, which also aligns with Roßnagel's recent observations[23]. Consistently with EDPS v SRB, the assessment should distinguish actual or reasonably foreseeable transfers involving recipients with relevant means of identification from speculative chains of disclosure lacking a demonstrable likelihood of occurring.

The "means reasonably likely to be used" assessment should fall back on realistic capacities rather than speculative occurrences

While the draft Guidelines refer to *all* objective factors when assessing the means reasonably likely to be used to identify a data subject, they should more explicitly and consistently reflect the full reasoning of the CJEU in Breyer. Paragraph 26 appropriately recognises that identification may not be reasonably likely where it is prohibited by law, practically impossible or dependent on disproportionate effort in terms of time, cost and labour. However, the operational assessment in paragraph 29 should reflect more consistently the distinction drawn in Breyer, paragraphs 45-49, between the existence of a conceivable means of combining information and the realistic likelihood of that means being used in the circumstances of the case. Accordingly, a merely theoretical possibility of identification should not in itself preclude anonymity where, in the circumstances of the case, the risk of identification is de facto negligible.[24]

By contrast, the draft Guidelines place particular emphasis on the existence of legal channels through which additional information may be obtained (last sentence of paragraph 29). While this reflects the facts that led the CJEU to conclude that the

[23] Professor Dr Alexander Roßnagel, Anonyme Datenverarbeitung: Dogmatische Schlussfolgerungen aus der Rechtsprechung des EuGH, 2026.
[24] Professor Dr Alexander Roßnagel, Anonyme Datenverarbeitung: Dogmatische Schlussfolgerungen aus der Rechtsprechung des EuGH, 2026.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

dynamic IP addresses at issue in Breyer constituted personal data (paragraphs 47-49 of the judgment), the Guidelines would benefit from placing equal emphasis on the *objective legal test* laid down by the CJEU (paragraph 46 of the Breyer judgment). In particular, the statement that the existence of a legal route to additional information objectively establishes that such access constitutes a means reasonably likely to be used should be qualified. Legal availability is a relevant factor, but does not necessarily establish the practical accessibility, feasibility or reasonable likelihood of using that route in every case. The assessment should also consider the conditions governing access, the relevant actor's legal standing, the expected time and cost, the likelihood of obtaining the information and its suitability for successful identification.

For example, the theoretical existence of a legal procedure through which additional information could be obtained should not be treated as sufficient where the relevant entity lacks the legal standing, factual grounds or practical ability to invoke that procedure in the circumstances under assessment. Conversely, where a legal route is effectively available, routinely usable and capable of providing the necessary identifying information, it may constitute a relevant means of identification. FEDMA recommends clarifying that legal availability is an element of the contextual assessment, rather than an irrebuttable presumption of reasonable likelihood. As such, adopting a more objective approach would ensure that the assessment remains firmly anchored in the concept of realistic capacities rather than speculative occurrences.

Furthermore, paragraph 32 of the draft Guidelines correctly acknowledges that legal prohibitions can prevent identification and that compliance with the law may generally be presumed. Paragraph 33 further requires sufficient evidence of a concrete risk before that presumption may be displaced. However, the Guidelines should clarify how this evidentiary threshold is to be applied in practice, including which circumstances justify considering unlawful identification pathways and when such scenarios may reasonably be excluded. The mere existence of actors capable of violating the law should not, without objective evidence concerning access, capability and realistic likelihood, be sufficient to prevent information from being recognised as anonymous. FEDMA therefore recommends that the safeguards recognised in paragraphs 32–33 be reflected consistently throughout the assessment of third-party capabilities, identification chains and the illustrative examples.

The draft Guidelines also expand the factual analysis to include motivation, accidental identification, negligence, contractual safeguards and changes in technology over time (paragraphs 31–35). FEDMA recognises that these factors may be relevant in particular circumstances. However, paragraph 31 should clarify how the incentives, capabilities, practical obstacles and potential consequences of re-identification are to be assessed objectively, including where identification depends on several successive actions by

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

different parties. Furthermore, examples based on accidents or exceptional circumstances may, without clear criteria for assessing their likelihood, encourage an unnecessarily conservative approach, despite the Guidelines acknowledging that anonymity does not require eliminating all residual risk. In parallel, the draft Guidelines provide insufficient operational guidance on how undertakings should assess the *likelihood* of such scenarios occuring in reality. Paragraph 35 should also distinguish material changes that justify reassessment from remote technological possibilities that do not materially affect present identifiability. This may lead to confusion and inconsistent application of the GDPR. The assessment of "means reasonably likely to be used" should therefore remain more closely aligned with the objective factors laid down by the *CJEU* in case law, including Breyer case, and should exclude purely theoretical possibilities where the risk of identification is de facto negligible.[25] Moreover, the more operational approach illustrated by the UK ICO "motivated intruder test" could provide a useful methodological reference, without replacing the legal standard established by the GDPR and the CJEU.[26] Otherwise, companies and national data protection authorities may face difficulties in conducting consistent, objective and evidence-based assessments.

While it is understandable to illustrate, through examples, the range of entities that could contribute to identifying a data subject (paragraph 30), the identifiability assessment should primarily focus on the capacities of actors, insofar as those capacities constitute means reasonably likely to be used to identify a data subject, as the last sentences of paragraph 30 recognise. An excessive focus on categorising potential actors may increase complexity without necessarily improving the quality, consistency or predictability of the assessment. The granularity in the list provided in paragraph 30 has limited practical added value for companies conducting an objective and proportionate assessment. This is especially relevant because footnote 25 correctly acknowledges that not every potential actor needs to be considered systematically in every case. The Guidelines should therefore focus on a capacity-based assessment that identifies relevant actors by reference to their realistic access to the data, availability of auxiliary information, technical capabilities and plausible participation in identification pathways. This would provide a more objective, proportionate and operational framework for companies, particularly SMEs and cross-border service providers.

[25] Professor Dr Alexander Roßnagel, Anonyme Datenverarbeitung: Dogmatische Schlussfolgerungen aus der Rechtsprechung des EuGH, 2026.

[26] UK Information Commissioner's Office (ICO), Anonymisation Guidance, particularly the guidance on ensuring effective anonymisation and assessing re-identification risks. The ICO's methodology is cited as a comparative technical reference, not as an independent source of obligations under EU law.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

c. Additional considerations (mixed datasets and anonymisation as a data processing activity)

Personal and non-personal data should not automatically be treated alike

FEDMA supports guarantees ensuring that personal data remain protected where a dataset contains a mixture of personal and anonymous data. However, although paragraph 36 recognises that personal and anonymous components may be processed separately, the Guidelines should clarify the practical conditions and legal consequences of such separation. In particular, treating a mixed dataset as containing personal data for compliance purposes should not be confused with classifying every individual component of that dataset as personal data. The application of the GDPR to the processing of a mixed dataset does not, in itself, alter the legal nature of information that is anonymous. Where information within a dataset does not relate to an identified or identifiable natural person, assessed in the relevant context, its treatment should not automatically be determined by the existence of other records that remain personal. Moreover, the CJEU clarified in the SRB case that data can constitute personal data for one entity and anonymous data for another, depending on the circumstances and the means reasonably likely to be used by the relevant entities. A more granular approach would better reflect the contextual nature of identifiability and the distinction between personal and non-personal information. This distinction is also consistent with Article 2(2) of Regulation (EU) 2018/1807 on the free flow of non-personal data[27], which expressly addresses datasets containing both personal and non-personal information. That provision recognises the applicability of the Regulation to the non-personal component, while preserving the application of the GDPR where personal and non-personal data are inextricably linked. The Guidelines should reflect this legislative framework and provide practical criteria for determining when components can be effectively separated and assessed independently, without suggesting that the presence of personal data necessarily changes the legal classification of every other element of the dataset. FEDMA recommends clarifying that the status of data within mixed datasets should be assessed on the basis of identifiability and the means reasonably likely to be used, rather than being determined automatically by the existence of personal data elsewhere in the dataset. The Guidelines should provide practical examples of effective technical, functional and organisational separation, including appropriate access controls, independently accessible aggregate outputs and safeguards against

[27] Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, Article 2(2); European Commission, Communication COM(2019) 250 final, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

recombination, enabling anonymous components to be processed without unnecessarily extending GDPR requirements to those components.

The Guidelines should not include unnecessary barriers to effective anonymisation

FEDMA welcomes the clarification in paragraph 38 that anonymisation constitutes a data processing activity within the scope of the GDPR for as long as personal data are being processed, and that, where anonymisation forms part of the same processing activity and pursues the same purpose, the applicable legal basis should be presumed to coincide with that of the preceding processing, including, where relevant, the applicable condition under Article 9(2) GDPR.

However, the Guidelines would benefit from further clarification on the legal basis applicable to anonymisation. In particular, the EDPB should clarify that anonymisation does not require a new, independently established legal basis merely because it constitutes a distinct technical operation within an existing lawful processing activity pursued for the same purpose. Where anonymisation is undertaken for a different purpose, the applicable purpose-limitation and compatibility rules should be assessed, without presuming that the production of anonymous data necessarily constitutes incompatible further processing. This is particularly important because anonymisation is intended to strengthen the protection of personal data. An interpretation that unnecessarily complicates the implementation of effective anonymisation could discourage controllers from reducing the identifiability of the information they process and retain.

In many situations, anonymisation is not pursued as a separate objective but as a privacy-enhancing measure intended to reduce risks and to support compliance with GDPR obligations. In those cases, anonymisation should not automatically be treated as a new purpose or as incompatible further processing merely because it involves a distinct technical operation. Where anonymisation serves the purposes of an existing lawful processing activity, it may remain covered by the corresponding legal basis. Where it pursues a separate purpose, the applicable purpose-limitation and compatibility requirements must be assessed in the circumstances of the case. This is particularly relevant where anonymisation contributes to compliance with the principles of data minimisation and storage limitation under Articles 5(1)(c) and 5(1)(e) GDPR, or constitutes an appropriate measure for data protection by design and by default or security of processing under Articles 25 and 32 GDPR. This approach is further supported by Article 11(1) GDPR, which provides that, where the purposes of processing do not or no longer require identification, the controller is not obliged to maintain, acquire or process additional information solely to identify a data subject for the purpose of

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

complying with the GDPR[28]. Although Article 11 does not itself establish that information is anonymous, it confirms the Regulation's recognition that identification should not be preserved or introduced unnecessarily. Anonymisation methodologies and evidentiary expectations should therefore avoid creating incentives to retain identifiable source data or acquire additional identifying information where this is not otherwise necessary, particularly when equivalent and reliable assessment methods are available. The Guidelines would therefore benefit from explicitly recognising that anonymisation conducted as part of a controller's compliance with GDPR obligations can rely on Article 6(1)(c) GDPR as a legal basis, where the anonymisation operation is necessary to comply with an applicable legal obligation and the requirements of Article 6(3) GDPR are satisfied. The Guidelines should clarify the circumstances in which such obligations provide an appropriate legal basis, without suggesting that every anonymisation operation automatically qualifies under Article 6(1)(c). This would support legal certainty and consistent application of the GDPR across Member States.

In practice, data can also be collected for the specific purpose of producing anonymous data, with identifiable source data deleted once anonymisation has been effectively completed, which does not diminish the privacy-enhancing function intended to reduce risks for data subjects. Such data processing can generate societal, economic and innovation benefits. Those data processing activities should therefore also be incentivised, rather than discouraged. The Guidelines would therefore benefit from clarifying that Article 6(1)(f) GDPR may provide an appropriate legal basis for the collection and processing of personal data necessary to produce anonymous data, provided that a legitimate interest is established, the processing is necessary for that interest and the interests or fundamental rights and freedoms of data subjects do not override it. In line with paragraph 39, timely anonymisation, the prompt deletion of identifiable source data and effective safeguards should be recognised as relevant factors when assessing the impact on data subjects. Such clarification should preserve all other applicable GDPR requirements, including Article 9 where relevant, as well as applicable ePrivacy requirements, while promoting a consistent and proportionate approach across Member States.

[28] GDPR, Article 11(1), read together with Recital 57 and Articles 5(1)(c), 5(1)(e), 25 and 32.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

3. Technical analysis

The technical assessment should support, rather than replace, the GDPR legal test for anonymisation

FEDMA welcomes the EDPB's effort to offer a structured technical framework for assessing whether anonymisation is effective. A rigorous assessment of disclosure risks is indispensable, particularly where granular datasets or accessible auxiliary information create a realistic possibility of identifying individuals. However, technical indicators must remain instruments for applying the legal definition of personal data, not additional independent conditions of anonymity. The applicable test remains Article 4(1) and Recital 26 GDPR, assessed from the relevant perspective and by reference to means reasonably likely to be used for identification[29].

The three criteria of No Record Isolation, No Linkage and No Inference reflect established lines of analysis in the Article 29 Working Party's Opinion 05/2014[30]. They identify different potential disclosure mechanisms, but their technical application is dependent on the data, the recipient, the disclosure environment, the auxiliary information realistically available and the particular attack under consideration. Accordingly, the Guidelines should recommend that assessments state their threat model expressly: the information assessed, the relevant actor, the identification objective, access conditions, supplementary data, foreseeable time horizon, technical capabilities, safeguards and evidence of potential success. This would make conclusions reviewable and comparable without requiring a uniform technical solution for every dataset.

FEDMA particularly welcomes the distinction between the contextual and simplified approaches in paragraphs 45-49. Paragraph 48 recognises that the simplified approach is voluntary and can classify information more conservatively than the applicable legal standard. Paragraph 52 likewise makes clear that failing one criterion does not, without further analysis, establish that information is personal data. These qualifications should be repeated alongside the decision table in paragraph 97 and the explanatory flowchart: a failed preliminary technical test must not be treated as conclusive proof of identifiability, nor should a properly substantiated contextual assessment be regarded as deficient merely because it follows a different method.

The Guidelines should avoid creating an asymmetry whereby controllers are encouraged to apply a deliberately more conservative methodology while the legal status of the same information must ultimately be determined by the contextual test established by the

[29] Regulation (EU) 2016/679 (GDPR), Article 4(1) and Recital 26; CJEU, Breyer, C-582/14, judgment of 19 October 2016, paras 45–49; EDPS v SRB, C-413/23 P, judgment of 4 September 2025, paras 75–89.
[30] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216), adopted 10 April 2014; EDPB, Guidelines 02/2026 on Anonymisation (draft for consultation), paras 43–53.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

GDPR. A simplified methodology may serve as an optional operational tool, but it should not be treated as an equivalent legal standard or become a preferred benchmark against which a properly substantiated contextual assessment is judged.

Simplification should facilitate compliance with the applicable legal test, not substitute a stricter substantive threshold. The risk of false negatives expressly acknowledged in paragraph 48 is not without consequences: treating anonymous data as personal may unnecessarily restrict its lawful use and reuse, discourage investment in effective anonymisation techniques and generate additional compliance costs without a demonstrated improvement in the protection of individuals. In particular, an organisation's decision not to use the simplified approach, or to depart from its preliminary findings, should not create an adverse presumption concerning the effectiveness of anonymisation. The relevant question must remain whether identification is reasonably likely in the actual circumstances, rather than whether the controller has followed the most conservative available methodology.

The assessment should also recognise that anonymisation can form part of data protection by design and by default under Article 25 GDPR, through data minimisation, restricted access, aggregation and appropriately configured privacy-enhancing technologies (PETs). Techniques such as differential privacy, controlled query interfaces, synthetic-data generation, secure computation and data clean rooms may contribute relevant safeguards, depending on their configuration; none automatically renders personal data anonymous[31]. The Guidelines should be technologically neutral, accept equivalent and demonstrably effective safeguards, and distinguish the processing of identifiable source information from the status of anonymous outputs.

More generally, the EDPB tends to rely on hypothetical use cases rather than on concrete empirical ones. The final guidelines should make a reference to the "From pseudonymous to anonymous data" report which describes concrete European industry use-cases on data anonymisation across sectors.[32] The report shows that:

(1) The threshold for pseudonymised data to qualify as anonymous is in practice very high;

(2) Achieving anonymisation requires layered safeguards, combining technical, organisational and contractual measures; and

[31] GDPR, Article 25; EDPB, Guidelines 02/2026, paras 39, 83–88; ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of techniques; ISO/IEC 27559:2022, Privacy enhancing data de-identification framework.

[32] Dr. Rob van Eijk and Benjamin de Vanssay, From pseudonymous to anonymous data, June 2026 (weblink).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

(3) Identifying recurring patterns and effective safeguards can support the definition of clear, operational criteria to determine when pseudonymised data becomes anonymous.

The distinction between technical evidence and legal classification should be reflected in every adverse conclusion arising from the three criteria.

The distinction between technical evidence and legal classification should be reflected in every adverse conclusion arising from the three criteria. Where a technical assessment identifies a potentially successful disclosure mechanism, the Guidelines should require a reasoned explanation of how the demonstrated mechanism relates to a natural person and establishes identification or identifiability under Article 4(1) and Recital 26 GDPR. A technical result should not be regarded as legally decisive merely because it exceeds an illustrative risk parameter or fails a preferred assessment method. Equally, sufficiently reliable evidence of an actual identification pathway cannot be dismissed by relying on a general claim that the output was intended to be anonymous.

a. The three criteria

The three criteria should be complementary technical tests, not cumulative legal requirements

FEDMA supports retaining No Record Isolation, No Linkage and No Inference as complementary technical questions. Each tests a distinct route through which information may become attributable to an individual. The criteria should not, however, be presented as three self-standing legal definitions. In the EDPB's own framework, satisfying all three criteria supports a finding of anonymity, whereas a preliminary failure must be examined in accordance with paragraphs 95–103 and, where relevant, through the contextual approach. In particular, the consequences of an established, specific and meaningful inference must be distinguished from the initial identification of a hypothetical inference technique.

The Guidelines should resolve the apparent ambiguity concerning the cumulative operation of the three criteria. Their simultaneous satisfaction may provide a sufficient basis for a positive conclusion under the EDPB's assessment framework; however, the failure of one criterion does not necessarily preclude anonymity. Accordingly, the three criteria cannot be treated as cumulative legal conditions that must invariably be satisfied before information can be recognised as anonymous. They are complementary technical tests whose results must be assessed according to their legal significance.

This distinction is not merely terminological. If failure of an individual criterion can coexist with anonymity, presenting the criteria as necessary cumulative requirements

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

risks creating a de facto standard stricter than Article 4(1) and Recital 26 GDPR. FEDMA therefore recommends that paragraphs 46 and 52, the outcome table in paragraph 97 and the accompanying flowchart expressly distinguish between the joint satisfaction of technical criteria as a sufficient assessment outcome and the legal requirements necessary for determining identifiability.

Provide a proportionate and documented assessment framework, rather than mandatory thresholds or certification

To promote operational consistency, FEDMA recommends a proportionate, documented assessment structured around five questions:

(i) what precise dataset or output is being assessed and which natural persons could be concerned;
(ii) whose perspective, access and legal role are relevant;
(iii) what record isolation, linkage or inference techniques are realistically available in that setting;
(iv) how reliable and consequential could their use be, taking account of existing controls; and
(v) do the resulting facts establish identification or identifiability through means reasonably likely to be used? These questions should be accompanied by worked examples and an evidence checklist, not transformed into a mandatory certification procedure or a universally applicable numerical threshold.

Technical evidence should be assessed contextually and according to the nature, reliability and operational relevance of the technique concerned

Technical evidence should be evaluated according to the nature of the technique. Relevant indicators may include record or population uniqueness; the accuracy and coverage of linkage; false-positive and false-negative rates; inference confidence against a meaningful baseline; sensitivity to individual contributions; accessible auxiliary sources; and the effectiveness of disclosure controls. Even a successful laboratory demonstration against a different dataset does not, without contextual analysis, establish that the same identification pathway is reasonably likely in operational use. Equally, strong empirical evidence of realistic identification cannot be disregarded merely because a dataset is labelled “aggregated”, “synthetic” or “privacy-preserving”.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

b. No Record Isolation

Record uniqueness should be an indicator, not proof of identifiability

Paragraphs 54-58 describe the risk arising from a unique combination of attribute values relating to a single individual. FEDMA agrees that unusual or highly granular records can create identification risks. However, uniqueness within a released sample is not equivalent to uniqueness within the relevant population, and neither is automatically equivalent to the identification of a natural person. The operational assessment should distinguish record uniqueness, the availability of corresponding attributes outside the dataset and the realistic possibility of matching a unique record to an individual[33].

This distinction is already supported by paragraphs 98-100 and example 24, where survey responses may be unique without permitting identification of respondents. FEDMA recommends that this important qualification be stated alongside the description of the criterion in paragraphs 54-57, rather than appearing only at the final stage of the assessment. A unique record should trigger further contextual examination where appropriate; it should not create a presumption that a unique person can be singled out through means reasonably likely to be used.

In practice, the risk depends on factors such as the attributes' granularity and stability, the size and composition of the sample and target population, the knowledge available to prospective recipients, the presence of persistent identifiers and the purpose and conditions of disclosure. An unusual combination of answers in a confidential consumer survey may remain unattributable to any respondent. By contrast, a unique sequence of high-resolution location observations may support effective recognition and profiling of a natural person and should be assessed accordingly.

The Guidelines should also avoid treating a single minimum group size or a particular k-anonymity configuration as a universal legal condition

The Guidelines should also avoid treating a single minimum group size or a particular k-anonymity configuration as a universal legal condition. Such measures may be technically useful in defined contexts, but the appropriate parameter depends on the dataset, the attack model, attribute diversity and the actual disclosure setting. FEDMA recommends examples demonstrating both a unique record that remains anonymous and a non-unique or grouped record that nevertheless exposes an identifiable individual.

The Guidelines should therefore make explicit that record uniqueness is a technical indicator, not an independent legal threshold. If the EDPB itself accepts that a unique

[33] EDPB, Guidelines 02/2026, paras 54–58 and 98–100, particularly Example 24; Khaled El Emam and Luk Arbuckle, Anonymizing Health Data: Case Studies and Methods to Get You Started (O'Reilly Media, 2013), relevant discussion of uniqueness and re-identification risk.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

record may remain anonymous, the absence of record isolation cannot logically be a necessary legal condition for anonymity. Its relevance must depend on whether the uniqueness can realistically contribute to identifying a natural person through means reasonably likely to be used.

c. No Linkage

There should be a consistent distinction between technical linkability, reliable matching of records relating to the same person, and the identification or identifiability of that person.

FEDMA recognises that joining information across datasets may reveal associations that are not apparent in the original data. Paragraph 60 rightly refers to records relating, with certainty or high likelihood, to the same individual; paragraphs 101-103 further acknowledge that linkage does not necessarily result in identification. The Guidelines should preserve this distinction consistently: a technically possible association between records, a reliable match referring to the same natural person and the identification of that person are related but separate questions.

Linkage should be assessed by reference to the relevant actor's realistic ability to access and use the additional information, rather than the mere existence of technical linkability with another dataset.

Moreover, the existence of a technically linkable dataset does not, in itself, establish that the linkage is reasonably likely to be performed by the relevant entity or that the resulting information permits the identification of a natural person. The legal assessment should not depend on the formal existence of another dataset, but on the identification capabilities realistically arising from the available information and processing circumstances. If linkage does not enable identification through means reasonably likely to be used, it cannot, by itself, determine that anonymity has been lost.

A meaningful linkage assessment should identify the additional datasets and join attributes at issue, the relevant entity's realistic ability to obtain or use them, the quality and stability of the matching variables, the expected coverage and accuracy of the matching method, and the likelihood that the resulting combination will identify an individual. Where probabilistic matching is used, the assessment should take account of false matches, uncertainty, relevant base rates and whether an asserted high match score is sufficient to associate records reliably with the same natural person. Technical accuracy must be considered together with access, cost, time and the means reasonably likely to be used under Recital 26[34].

[34] EDPB, Guidelines 02/2026, paras 59–65 and 101–103; GDPR, Recital 26; CJEU, Breyer, C-582/14, paras 45-49.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Actual access conditions, contractual restrictions, technical segregation and other effective safeguards should be considered when determining whether linkage is reasonably likely

The availability of an external dataset on the internet does not necessarily mean that it is realistically usable for identification by every recipient. Equally, data held by a commercial intermediary, an affiliated controller or another actor may be highly relevant where access, a contractual arrangement or an established matching process makes linkage foreseeable. Contractual restrictions, technical segregation and controlled outputs may reduce the likelihood of linkage, but cannot automatically overcome demonstrable identification capabilities.

For example, joining event-level marketing/advertising data with identifiable customer records within a controlled measurement environment may constitute processing of personal data and must comply with the GDPR and, where applicable, the ePrivacy framework. The anonymous aggregate campaign statistics subsequently released from that environment should be assessed separately, in light of their granularity, query controls, accessible auxiliary information and the actual capabilities of recipients. A data clean room is not anonymous merely because it is described as such; the status of each input, processing operation and output requires its own assessment.

d. No Inference

The ability to derive general statistical or predictive information should be distinguished from a demonstrated specific and meaningful inference concerning an individual

The No Inference criterion requires particularly careful articulation because producing statistical knowledge is often the purpose of anonymisation. FEDMA welcomes the express recognition in paragraph 69 that personal data may be inferred from information that is not itself personal data, and the distinction in paragraphs 70-71 between general population-level information and specific, meaningful inferences about an individual. The mere ability to use aggregate statistics to make predictions about people, including persons absent from the source dataset, should not be equated with the disclosure of personal information about a contributor to that dataset.

The central legal distinction is between the status of the assessed information and the status of information subsequently inferred from it. An inference may generate personal data concerning an identified or identifiable individual without necessarily changing the legal classification of the information from which that inference was derived. The Guidelines correctly acknowledge this principle in paragraph 69; it should be reflected

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

consistently in the definition, application and consequences of the No Inference criterion, including the outcome table in paragraph 97.

In particular, the fact that anonymous data retains analytical or predictive utility cannot, by itself, justify its classification as personal data. The legal assessment must establish whether the inferred information is specifically and meaningfully connected to an individual through the assessed information and means reasonably likely to be used. The ability to derive useful statistical knowledge is not a substitute for the legal requirements of Article 4(1) GDPR.

The Guidelines should distinguish between different inference techniques and require their actual capacity to produce a specific and meaningful individual-level inference to be demonstrated

At the same time, FEDMA acknowledges that sufficiently granular statistical releases, small groups, repeated or overlapping queries, high-dimensional data and model outputs can, in some cases, disclose individual attributes or enable reconstruction. The relevant inquiry should identify the information inferred, the individual concerned, the causal or informational connection with the assessed dataset, and the means reasonably likely to be used to obtain a specific and meaningful result. Examples 13 and 14 help distinguish generalised statistical predictions, while example 16 illustrates a disclosure arising from the combination of aggregate salary figures.

Marketing example
Marketing departments often rely on anonymised granular-statistics to gain insight into their customers and markets. Although the source data relate to individuals, statistical techniques are used to extrapolate this information to the whole dataset or to a specific market, and the results are made available only at a micro-aggregated level. For geographic aggregation, for example, each aggregated unit typically covers at least four households (or ten persons), and the data are never provided below this threshold. This ensures that the statistics cannot reveal information about any single individual. Marketers use such micro-aggregated statistics, for example on purchasing power or car ownership, to help predict which people are likely to be interested in their products or services. This example satisfies the No Inference criterion.

The Guidelines would benefit from distinguishing several technically different phenomena: attribute inference (predicting an individual characteristic), membership inference (determining whether an individual contributed to training or source data),

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

reconstruction or differencing attacks (recovering individual-level values), and model or output extraction. For each technique, an assessment should explain the attacker's objective, the relevant reference population, auxiliary information, success rate, uncertainty, validation method and whether the demonstrated output actually satisfies the specific-and-meaningful inference standard. A generic statement that an AI model or aggregate output "may leak information" is not an adequate substitute for these particulars[35].

A specific inference should not presuppose the identification or identifiability it seeks to establish

Moreover, the definition of a specific inference in paragraph 67 should not be applied in a manner that presupposes the very identification or identifiability which the assessment is intended to establish. The assessment should demonstrate the existence of the relevant individual, the connection between the inferred information and that individual, the dependence of the inference on the assessed information and the realistic effectiveness of the technique. The possibility that inferred information may affect an individual's rights or interests is relevant to the significance of an inference, but does not independently establish that the individual is identifiable.

FEDMA recognises that paragraph 87 already requires sufficient accuracy and confidence in the circumstances. The Guidelines should make that requirement operational through proportionate, context-sensitive evidentiary criteria, rather than introducing a universal numerical confidence threshold or allowing speculative inference capabilities to determine the legal status of information.

A counterfactual test should not require organisations to retain, reconstruct or reacquire identifiable source data where another technically reliable method can establish the relevant facts

FEDMA also welcomes the alternatives expressly contemplated in paragraph 71 for demonstrating whether an inference depends on an individual's contribution. However, the comparison of outputs generated from original dataset D and a modified dataset D', from which one person's records have been removed, cannot be universally practicable. Performing such a counterfactual analysis may require significant technical resources, computational infrastructure and specialist expertise, as well as substantial staff time to reconstruct datasets, rerun processing operations and evaluate the resulting outputs. Such capabilities may not be readily available to all organisations, particularly SMEs. Reconstructing the original dataset, repeating costly transformations or retaining

[35] EDPB, Guidelines 02/2026, paras 66–82, particularly paras 67–71 and Examples 13–16; Article 29 Working Party, Opinion 05/2014 (WP216), discussion of inference and linkage.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

identifiable source records solely to facilitate such a test may conflict with data minimisation and storage limitation. Counterfactual testing should therefore remain an optional evidentiary method, alongside provenance analysis, validated statistical testing, formal privacy guarantees, independent auditing and other technically appropriate approaches, especially after the source data have been irreversibly deleted.

The Guidelines should further clarify that evidentiary expectations must remain compatible with Articles 5(1)(c), 5(1)(e) and 11 GDPR. In particular, organisations should not be expected to reconstruct, reacquire or retain identifiable source information solely to perform a preferred counterfactual assessment where an alternative method can provide sufficiently reliable evidence of effective anonymisation. The acceptability of such alternatives should depend on their demonstrated technical effectiveness, rather than on formal adherence to a particular testing architecture.

Properly calibrated differential privacy, contribution bounding, output suppression, query budgets and other statistical disclosure controls may provide relevant evidence about individual disclosure risk. Such methods require adequate parameterisation, accounting for repeated releases and an understanding of the trade-off between utility and protection; they should not be treated as automatic legal safe harbours. Equally, the Guidelines should not imply that a disclosure risk is established merely because a sufficiently determined attacker might, in abstract terms, devise a future inference technique[36].

A failure of No Inference should not automatically determine the legal status of the data without demonstrating a specific and meaningful individual disclosure

Finally, the outcome table in paragraph 97 should be read together with the conditions defining a specific and meaningful inference in paragraphs 67-71 and the requirement to assess relevant perspectives. Where an inference has been objectively demonstrated to satisfy those conditions through means reasonably likely to be used from a relevant perspective, a finding that information is not anonymous may follow; the mere naming of a possible inference attack does not establish that its conditions have been met. FEDMA recommends inserting this distinction directly into the table's explanatory notes and providing contrasting examples of population-level inference, meaningful individual disclosure and unsuccessful speculative attacks.

[36] EDPB, Guidelines 02/2026, para 71 and footnotes 43–44; Cynthia Dwork and Aaron Roth, The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science 9(3–4) (2014), pp. 211–407.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

In particular, the Guidelines should explain why a failure of No Inference under the contextual approach necessarily establishes a legally relevant disclosure in the circumstances assessed, and should distinguish a demonstrated individual-specific disclosure from statistical prediction, probabilistic association or the identification of a conceivable attack technique. Where the technical criterion is considered conclusive, the conditions making that result legally conclusive should be expressly identified and supported by verifiable evidence.

4. The interplay between the legal and technical analysis

Technical findings should inform, but not replace, the legal assessment of whether information relates to an identified or identifiable natural person

FEDMA considers that the legal and technical sections should operate as one coherent assessment rather than as two potentially competing standards. The legal question—whether the information relates to an identified or identifiable natural person through means reasonably likely to be used—must determine the significance attributed to the technical findings, not the other way around. The three criteria are useful evidence of possible identification mechanisms; they do not independently amend Article 4(1) or Recital 26 GDPR[37].

To ensure that connection, FEDMA recommends that the Guidelines and the decision table in paragraphs 95-103 be accompanied by a consolidated decision sequence:

(1) define the exact information and processing operation;
(2) identify the relevant entity or entities, their legal roles and the applicable perspective;
(3) determine whether the information relates to a natural person by content, purpose or effect;
(4) identify realistic record-isolation, linkage and inference techniques;
(5) assess the relevant actors' means, auxiliary information, access conditions and safeguards against the objective factors of Recital 26;
(6) document which technical findings amount to an actual identification pathway and reach a reasoned conclusion; and
(7) determine proportionate triggers for reassessment.

This sequence should be a recommended, adaptable assessment aid rather than a new mandatory compliance procedure.

In applying that sequence, the Guidelines should emphasise that failure of No Record Isolation may still be compatible with anonymity where unique records cannot realistically be associated with individuals, as expressly recognised by example 24.

[37] GDPR, Articles 4(1) and 70(1)(e) and Recital 26; EDPB, Guidelines 02/2026, paras 45–53 and 95–103.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Failure of No Linkage should prompt examination of whether the combined information can identify a natural person, as paragraphs 101-103 already contemplate. No Inference should be assessed against its defined conditions of specificity, meaningfulness, dependence and applicable perspective; where these are actually met, the technical and legal conclusions should converge. The paragraph 97 table should therefore distinguish an initial technical warning, the required contextual follow-up and a substantiated legal conclusion, rather than allow those stages to be conflated.

Organisations should be free to apply the contextual approach directly, without first applying or failing the simplified approach

The choice between the simplified and contextual approaches is decisive in this respect. Paragraph 48 and footnote 36 correctly acknowledge that the simplified approach is voluntary, more conservative than the legal minimum in some cases, and cannot by itself be used by third parties to prove a GDPR violation. FEDMA requests that these safeguards be repeated in every flowchart and summary table, and that organisations be expressly permitted to rely on a documented contextual assessment without being required first to fail or complete the simplified approach.

The relevant perspective should also remain consistent with the judgment in EDPS v SRB. Data may be personal for an originating controller while being anonymous for an independent recipient who lacks means reasonably likely to be used for identification. The assessment must nevertheless consider actual or reasonably foreseeable onward transfers and the requirements attached to the relevant processing role; the recipient-relative approach should not be presented as automatically excluding processor obligations or responsibilities arising at the stage of collection[38].

The Guidelines should give practical effect to the safeguards they themselves recognise: paragraph 22 excludes negligible risks from the assessment; paragraphs 32-33 require objective evidence before unlawful conduct displaces the general presumption of legal compliance; footnote 25 to paragraph 30 excludes any systematic obligation to assess every conceivable actor; paragraph 35 recommends reassessment where possible and appropriate; and example 22 illustrates that the possibility of a data leak need not prevent a finding of anonymity. These qualifications should be consolidated into transparent criteria for relevance, exclusion of remote scenarios, proportional documentation and event-driven reassessment. Such an approach would recognise that the legal classification of information may change where the relevant circumstances

[38] CJEU, EDPS v SRB, C-413/23 P, judgment of 4 September 2025, paras 75–89 and 99–115; EDPB, Guidelines 02/2026, paras 15 and 20–21.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

materially change, without treating the possibility of such a future change as sufficient, in itself, to prevent a present finding of anonymity.[39]

Compliance should be demonstrable through different scientifically sound and contextually appropriate methods, rather than a single prescribed methodology or technical threshold

The practical application of technical criteria should also be consistent with legal certainty, technological neutrality and proportionality. Organisations should be able to demonstrate compliance through different scientifically sound and contextually appropriate methods, provided that those methods establish the applicable legal requirements. The EDPB should avoid presenting a particular assessment methodology, technical parameter or precautionary margin as a universal prerequisite where the GDPR does not establish such a condition.

This does not prevent supervisory authorities from requiring specific corrective measures where the facts and applicable legal powers justify them. However, case-specific supervisory requirements should be distinguished from generally applicable conditions for recognising anonymity. In particular, differences in national technical preferences should not result in materially divergent legal classifications of equivalent processing circumstances without an objective and legally justified basis.

These activities involve different data sources, technical capabilities, disclosure environments and identification risks. Their assessment should distinguish personal-data processing that remains subject to the GDPR from statistical or analytical outputs that may qualify as anonymous. A sector-wide approach would also help avoid the assumption that commercial use of information necessarily entails a meaningful incentive to re-identify natural persons.

FEDMA therefore recommends a short operational annex containing a proportionate threat-model template; a non-exhaustive checklist of relevant objective factors; examples of defensible evidence for each technical criterion; a decision table explicitly separating technical indicators from legal classification; and practical scenarios covering controlled sharing, public release, statistical reporting, research and marketing. This would support consistent enforcement and SME compliance, preserve the protection of individuals, and facilitate the lawful use of anonymous data without creating additional substantive legal standards or universal numerical thresholds.

[39] Professor Dr Alexander Roßnagel, Anonyme Datenverarbeitung: Dogmatische Schlussfolgerungen aus der Rechtsprechung des EuGH, 2026.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Such guidance should also clarify the expected standard of evidence for different assessment scenarios. In particular, the nature and extent of technical testing, documentation and reassessment should correspond to the relevant identification risks, data characteristics and disclosure conditions. Organisations should be able to rely on reproducible testing, validated technical methods, documented safeguards and other reliable evidence appropriate to the circumstances, without being required to demonstrate the absolute impossibility of identification or to investigate every conceivable future attack. Consistent with the GDPR's broader risk-based approach, the nature and extent of technical testing, documentation and reassessment should correspond to the relevant identification risks, data characteristics and disclosure conditions.

FEDMA further encourages the EDPB to assess, in dialogue with stakeholders, the practical implications of the proposed methodologies for SMEs and independent data-service providers, including their implementation costs, the availability of technical expertise and the feasibility of applying the criteria across different processing environments.

5. Societal, economic and competition implications

Effective anonymisation has important societal and economic functions. It can enable organisations to produce statistical information, conduct research, measure the effectiveness of services and commercial activities, improve products and support evidence-based decisions while reducing the need to retain or disclose identifiable information. These functions can benefit individuals directly through reduced exposure to personal-data risks and indirectly through research, innovation, competition and the availability of useful services.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Marketing example

- Anonymous purchasing and service-use trends can help businesses understand changing consumer needs, improve products and services, identify gaps in the market and make better-informed decisions about where products and services are made available.
- Independent market research based on anonymous data can similarly provide SMEs and new market entrants with insights into broader market developments that they could not generate from their own limited customer base, supporting competition and consumer choice.

These are precisely the types of responsible, privacy-preserving uses of data that should be facilitated by an approach consistent with the EDPB's Helsinki commitments to practical compliance, responsible innovation and European competitiveness.

The GDPR should not be interpreted as establishing an inherent conflict between protecting individuals and enabling lawful economic activity. Its objectives include the protection of natural persons and the free movement of personal data. Recital 4 expressly requires a proportionate balancing of the right to data protection with other fundamental rights, including the freedom to conduct a business[40]. The protection of individuals remains essential, but legitimate economic interests and the contribution of responsible data use to societal welfare should not be considered legally irrelevant.

These considerations are particularly urgent in the present European economic context. The European Commission's 2025 Competitiveness Compass expressly acknowledges that the Union has fallen behind the United States in advanced technologies, while China has caught up in several sectors and is taking the lead in emerging areas[41]. The Draghi Report similarly identifies innovation deficits, regulatory fragmentation and obstacles to business growth as structural challenges to Europe's prosperity[42]. Against this background, regulatory choices that may increase the cost, uncertainty or practical difficulty of developing privacy-preserving technologies deserve careful examination. Europe cannot afford to create unnecessary barriers to the responsible use of information while competing economies accelerate investment, technological development and market expansion.

From an economic perspective, the legal treatment of anonymisation can affect the costs of developing, sharing and using statistical and analytical information. Requirements involving specialised technical expertise, extensive documentation,

[40] GDPR, Recitals 2 and 4 and Article 1; Charter of Fundamental Rights of the European Union, Articles 8, 16 and 52(1).
[41] European Commission, A Competitiveness Compass for the EU, COM(2025) 30 final, 29 January 2025.
[42] Mario Draghi, The Future of European Competitiveness, Part A, 9 September 2024, particularly pp. 29–30 and 68–69.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

repeated reassessments or the evaluation of remote identification scenarios may generate significant fixed costs. Such costs can be especially challenging for SMEs and new market entrants, while larger organisations may be better able to distribute them across established compliance infrastructures and multiple services.

The consequences of regulatory uncertainty and unnecessary administrative burdens extend well beyond corporate compliance budgets. Businesses create employment, generate income, invest in innovation and contribute to the economic resources on which Europe's social model depends. When avoidable barriers prevent an undertaking from growing, delay the development of a service or discourage investment, the potential costs may ultimately be borne by employees, consumers, entrepreneurs and future generations. These consequences should not be dismissed as merely private commercial concerns. They are legitimate societal considerations that deserve attention when assessing the practical effects of regulatory interpretation.

Moreover, independent service providers may depend on access to appropriately anonymised information for market research, audience measurement, independent campaign verification and the development of innovative analytical products. If uncertainty concerning the recognition of anonymity unnecessarily restricts the supply or use of such information, it may create barriers to entry or reinforce informational advantages enjoyed by established operators. These effects should be assessed empirically rather than presumed, and legitimate compliance costs necessary to protect individuals must be distinguished from incremental costs arising from unnecessarily restrictive methodologies.

This concern is consistent with the European Union's wider policy objectives. The Draghi Report identifies regulatory fragmentation, compliance costs and obstacles to the growth of innovative European businesses as structural challenges to competitiveness[43]. The Digital Markets Act also recognises the importance of effective access to certain data and verification mechanisms, including the anonymisation requirements established by Article 6(11)[44]. These instruments do not lower the standard of protection required by the GDPR, but they demonstrate the importance of maintaining coherence between effective data protection, competition and the functioning of the internal market.

Importantly, these concerns are not external to the EDPB's own institutional commitments. In its Helsinki Statement of July 2025, the Board expressly committed to

[43] Mario Draghi, The Future of European Competitiveness, Part A, 9 September 2024, particularly pp. 29–30 and 68–69.
[44] Regulation (EU) 2022/1925 (Digital Markets Act), Article 6(8) and (11) and Recital 61; Regulation (EU) 2018/1807, Article 2(2).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

clearer and more practical guidance, easier compliance for micro, small and medium-sized organisations, responsible innovation and stronger European competitiveness[45]. These commitments should be reflected in the final Guidelines. It would be difficult to reconcile them with an approach under which voluntary precautionary methodologies, speculative identification scenarios or disproportionately demanding evidentiary expectations effectively become default compliance requirements, without a clear demonstration of their necessity under the GDPR and their additional protective value.

FEDMA therefore recommends that the EDPB consider the operational and economic implications of its proposed methodologies, particularly their effects on SMEs, market entry, independent measurement, research and cross-border data services. The final Guidelines should distinguish the costs inherent in satisfying the GDPR's legal requirements from additional costs associated with precautionary or voluntary methodologies, and should promote proportionate, technologically neutral and evidence-based means of demonstrating effective anonymisation.

Where the Guidelines recommend approaches that are more conservative than the legal standard, FEDMA calls on the EDPB to explain their expected additional protective benefits, the evidence supporting the relevant identification risks and the availability of less burdensome methods capable of providing equivalent protection. Such transparency is essential to informed stakeholder scrutiny and proportionate implementation. **The independence and technical authority of supervisory bodies do not make the practical consequences of their recommendations irrelevant; rather, those qualities make clear, accountable and evidence-based reasoning particularly important.**

Ultimately, enabling the responsible production and use of anonymous data is not a departure from data protection. When properly implemented, it is one means of protecting individuals while supporting economic and social activities that contribute to their welfare.

Europe should not be forced to choose between protecting fundamental rights and remaining economically competitive. The challenge for its institutions is to achieve both within the framework established by Union law. An interpretation that imposes unnecessary barriers to effective anonymisation risks undermining that objective, potentially discouraging privacy-enhancing innovation without delivering a corresponding improvement in the protection of individuals.

[45] European Data Protection Board, The Helsinki Statement on enhanced clarity, support and engagement, adopted 2 July 2025.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

*****

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org