20/10/2026

EFAMRO and Esomar Consultation Response to the European Data Protection Board Anonymisation Guidelines

EFAMRO the European Federation of Associations of Market Research Organisations. Founded in 1992, EFAMRO represents the interests of market, opinion and social research in Europe. Its members are national trade associations for research businesses.[1]

Esomar the worldwide, not-for-profit membership organisation committed to empowering and connecting the research, insights, and analytics community since 1947. Today, Esomar represents and provides connections among 50,000+ individuals and 750+ companies in 130+ countries.[2]

EFAMRO and Esomar represent the research and insights sector, accounting for a reported annual turnover of €34.87 billion in Europe.

1. About Market, Opinion and Social Research

1.1. Market research is comprised of all forms of market, opinion, and social research (herein referred to as "Market Research").

1.2. Market Research is the systematic gathering, analysis and interpretation of information about individuals or organisations. It uses the statistical and/or analytical methods and techniques of the applied social, behavioural, data and other sciences to generate insight and support decision making by providers of goods and services, governments, non-profit organisations and the general public.

1.3. Market Research stands at the heart of well-informed commercial, social and political decisions. Its purpose is to deliver information and insights about people's behaviour, needs and attitudes to inform decision making by providers of goods and services, governments, individuals, and society at large. Insight into what makes the success of a product, business initiative, consumer behaviour or government policy strategy is often the hidden – yet defining – factor that determines success and failure. It is our sector that provides the deeper intelligence needed for our world today by representing citizens' authentic voices, from all levels of society, in an unbiased and representative way by applying the tenets of statistical and scientific methods.

1.4. Market Research associations apply a comprehensive framework for self-regulation to ensure that researchers meet their ethical, professional, and legal responsibilities to the individuals whose data they use in research and to the clients and organisations which commission research. Members subscribe to self-regulation schemes that protect respondents' and participants' rights.

2. Purpose of our Response

Our associations welcome the European Data Protection Board's (EDPB) initiative to provide greater legal clarity on the anonymisation of personal data, particularly in light of evolving

[1] For more about EFAMRO see: https://efamro.eu/
[2] For more about Esomar see: https://esomar.org

technologies, the increasing use of artificial intelligence (AI) and recent case law of the Court of Justice of the European Union (CJEU).

2.1. Anonymisation is of fundamental importance to the market, opinion and social research sector. It enables research organisations to produce valuable insights, statistics and evidence for businesses, public authorities and society, while protecting the privacy and rights of individuals. A clear, proportionate and legally sound framework for assessing anonymisation is therefore essential to maintaining public trust and supporting responsible research and innovation.

2.2. Our associations particularly welcome the recognition that anonymity is contextual rather than an absolute property of data. Whether information constitutes personal data depends on the circumstances, including the entity assessing the data, the information available to that entity, the context in which the data are processed and the means of identification that are reasonably likely to be used. Consequently, the same dataset may be anonymous in the hands of one entity while remaining personal data in the hands of another that has access to additional information or different means of identification.

2.3. This approach reflects the practical realities of research supply chains, in which research organisations, data processors, clients and other organisations may hold different information and undertake different responsibilities. It also supports a more nuanced understanding of the relationship between anonymisation, pseudonymisation and personal data under the General Data Protection Regulation (GDPR).

2.4. Our associations broadly support the direction of the Guidelines and the proposed framework for assessing anonymity. However, we recommend a number of clarifications to ensure that the final Guidelines preserve the contextual nature of the legal test, apply a proportionate and risk-based approach, recognise the legitimate requirements of research and avoid imposing an unnecessarily restrictive standard of anonymisation.

3. Contextual Anonymisation

3.1. Our associations strongly welcome the adoption of a contextual assessment model that takes account of the perspective of the recipient or other relevant entity assessing the data. This connects the Guidelines' response to recent CJEU case law with the practical distinction between anonymisation, pseudonymisation and personal data in research.

3.2. This approach is important because identifiability cannot be determined solely by examining a dataset in isolation. It depends on the circumstances of processing, including the information available to the relevant entity, the resources and technical capabilities at its disposal, the surrounding environment and the realistic likelihood of identification.

3.3. This is particularly relevant to market, opinion and social research. Research organisations frequently process personal data to conduct fieldwork, manage samples, validate responses and undertake longitudinal analysis, before producing anonymised datasets, aggregate results or statistical outputs for clients. The information available to a research organisation may differ materially from that available to its client, and the ability of each organisation to identify individuals may therefore differ.

3.4. Our associations support the recognition that research organisations should be able to assess identifiability from their own perspective where they determine their own purposes and means of processing, taking account of the information and resources reasonably available to them.

3.5. It is essential that the final Guidelines explicitly preserve the contextual approach as the operative legal standard under the GDPR and make clear that the assessment must reflect the actual circumstances of the relevant entity, rather than an abstract assessment of all theoretically possible means of identification.

Recognition of research ecosystems and processing chains

3.6. Our associations welcome the acknowledgement that organisations involved in a processing chain may hold different information and consequently reach different conclusions about whether particular data are identifiable.

3.7. This reflects the structure of modern research operations. Research organisations may retain contact information or sample-management records separately from research responses, while clients may receive only anonymised outputs or datasets that do not permit identification using the means reasonably available to them.

3.8. The legal status of information should not be assumed to be identical for every organisation simply because the organisations participate in the same project or processing chain. Equally, the contextual approach should not be interpreted as allowing identifiability risks to be disregarded where additional information or realistic means of linkage are available.

3.9. In effect, the final Guidelines should explain how the contextual assessment applies to different entities within research supply chains, including the importance of considering the recipient's access to additional information, contractual arrangements, technical controls and practical ability to identify individuals.

The No Record Isolation, No Linkage and No Inference framework

3.10. Our associations support the proposed three-part framework as a useful and technology-neutral methodology for assessing whether data can reasonably be considered anonymous.

3.11. The framework appropriately recognises that identification risks extend beyond the presence of direct identifiers. Individuals may also be identifiable through combinations of attributes, the linkage of records with other datasets or the inference of information about an individual from apparently non-identifying data.

3.12. For research organisations, this provides a practical structure for considering the principal risks associated with data release and use. It can support consistent assessments while remaining adaptable to different datasets, purposes and technological environments.

3.13. We particularly welcome the attention given to quasi-identifiers, data linkage and inference, as these are important considerations when evaluating the disclosure risks associated with research data. However, the framework should operate as an aid to applying the contextual legal test, rather than as an independent or universally determinative test of whether information constitutes personal data.

3.14. The EDPB should retain the three-part framework while clarifying that its application must remain contextual and proportionate. A criterion that is not satisfied should inform the assessment of identifiability, but the terminology and conclusions should distinguish between a technical assessment outcome and a finding that the GDPR has been breached.

4.Main areas for improvement

Preserve the contextual approach as the operative legal standard

4.1. Our associations recommend that the final Guidelines distinguish more clearly between the legal standard for assessing anonymity under the GDPR and any simplified methodology proposed to help organisations apply that standard.

4.2. The contextual approach is essential because identifiability depends on the circumstances of the relevant entity, including the means reasonably likely to be used to identify an individual. It allows the assessment to reflect differences in the data, processing purposes, recipients, available information and practical capabilities.

4.3. Simplified methodologies can be valuable, particularly for supporting consistent assessments and documentation. However, they should remain optional compliance tools. They should not become a *de facto* regulatory expectation or be interpreted as a mandatory checklist that every organisation must complete in every case.

4.4. An overly prescriptive approach could lead organisations to prioritise adherence to a particular methodology over a substantive assessment of the risks relevant to their circumstances. It could also produce disproportionate burdens where a simpler, well-evidenced assessment would be sufficient.

4.5. We recommend that the EDPB:

- Explicitly confirm that the contextual assessment of identifiability is the operative legal standard under the GDPR.
- Clarify that any simplified methodology is an optional tool for supporting compliance, not a separate or mandatory legal test.
- Permit other reasoned and documented methodologies where they adequately assess the relevant identification risks.
- Emphasise the substance and evidential basis of an organisation's assessment, rather than adherence to a single prescribed methodology.

Clarify the treatment of aggregate data and statistical outputs

4.6. We recognise that aggregation does not invariably prevent identification. Small groups, highly granular results, unusual combinations of attributes or the availability of additional information may, in certain circumstances, enable individuals to be identified or information about them to be inferred.

4.7. However, the Guidelines should present this issue in a balanced manner. Aggregation is also an important means of reducing identification risks and can result in information that is anonymous in the circumstances in which it is held or disclosed.

4.8. Therefore, we recommend that Clause 17 expressly acknowledge both possibilities. The discussion should make clear that aggregate data may be identifiable in particular circumstances, but may equally be anonymous where the characteristics of the output and the surrounding circumstances do not permit identification by means reasonably likely to be used. Clause 58, as referenced in the draft Guidelines, may provide a useful basis for ensuring consistency.

4.9. This distinction is particularly important to market, opinion and social research. Research findings commonly take the form of population-level statistics, aggregated responses, trends, segment-level insights and other outputs designed to describe groups rather than identify individuals.

4.10. The fact that such findings inform commercial decisions, public policy or predictive analysis does not, in itself, make them personal data. Their legal status must be assessed by reference to whether they relate to an identified or identifiable natural person in the relevant circumstances.

4.11. Our associations recommend that the EDPB:

- Amend Clause 17 to recognise explicitly that aggregate data may be identifiable in some circumstances but may equally constitute anonymous information.
- Ensure that Clauses 17 and 58 present a consistent and balanced account of aggregation.
- Clarify that aggregate research findings and statistical outputs should not be treated as personal data solely because they inform decision-making or support predictive analysis.
- Encourage a contextual assessment of group size, granularity, disclosure controls, auxiliary information and realistic linkage risks, rather than treating aggregation as either automatically sufficient or inherently insufficient to achieve anonymity.

4.12. Avoid a de facto zero-risk standard

4.13. Our associations are concerned that some elements prescribed in the Guidelines could be interpreted as requiring a degree of certainty that is neither practically achievable nor consistent with the GDPR's contextual approach to identifiability.

4.14. The GDPR requires consideration of the means reasonably likely to be used to identify an individual, taking account of relevant objective factors. This is not equivalent to requiring organisations to eliminate every hypothetical or conceivable re-identification scenario.

4.15. Advances in computing, AI and data analysis may create new technical possibilities for linking datasets or inferring information. However, the theoretical existence of a technique does not, by itself, establish that the technique is reasonably likely to be used in the circumstances concerned.

4.16. A zero-risk interpretation would make anonymisation an unattainable standard in practice. It could discourage the responsible use of statistical data and unnecessarily restrict research, innovation and the production of evidence for public benefit.

4.17. Our associations support appropriate attention to emerging technologies and the reassessment of risks where relevant circumstances materially change. The Guidelines should nevertheless distinguish between a theoretical possibility and a realistic means of identification, taking account of the practical circumstances in which the data are held, disclosed or used.

Apply a proportionate risk-based approach

4.18. Our associations support an approach in which the assessment and selection of anonymisation measures reflect the characteristics of the data, the intended purpose, the recipient and the circumstances of processing.

4.19. The measures appropriate for detailed individual-level records may differ significantly from those appropriate for aggregated research findings. Likewise, information released publicly may require a different assessment from information made available to a restricted recipient under appropriate technical, organisational and contractual controls.

4.20. The final Guidelines should avoid creating an expectation that organisations must continually adopt the newest or most sophisticated anonymisation techniques irrespective of the risks involved. The existence of a new technique does not, by itself, establish that its adoption is necessary or proportionate in every case. This is particularly relevant to small and medium-sized enterprises (SMEs) and smaller research organisations, which may have limited resources for specialist technical expertise, extensive assessments or the implementation of advanced techniques. Their obligations under the GDPR remain applicable, but guidance should enable them to determine appropriate measures on the basis of a reasoned assessment rather than an open-ended expectation to implement every available solution.

4.21. The EDPB should also clarify that the scope and frequency of reassessment under the contextual approach should be proportionate to the identification risks and relevant changes in circumstances, rather than requiring continuous re-evaluation of every criterion irrespective of risk. Relevant material changes should prompt reassessment, with organisations documenting the basis for their review arrangements.

4.22. Proportionality should not be understood as a reduction in the protection required. It should ensure that the measures selected are appropriate to the actual circumstances and risks, and that organisations can explain and document the basis for their decisions.

Recognise the requirements of longitudinal and academic research

4.23. Our associations recommend that the Guidelines more explicitly recognise that full anonymisation is not appropriate at every stage of every legitimate research project.

4.24. For example, longitudinal research, panel studies and certain academic research methodologies depend on the ability to link responses from the same participant over time. Some projects also require controlled re-contact to invite participants to subsequent research waves, validate information or investigate changes in attitudes and behaviour.

4.25. Removing all possibilities of linkage or re-identification at the outset may undermine the scientific validity and practical feasibility of these methodologies. In such circumstances, strong pseudonymisation may be an appropriate safeguard. Identifiers can be replaced with codes, while the additional information needed to identify participants is kept separately and protected through appropriate access restrictions, security measures and governance arrangements.

4.26. The final Guidelines should explicitly recognise that controlled re-identification, participant re-contact and linkage over time may be necessary for longitudinal and academic research, and that strong pseudonymisation may be appropriate where full anonymisation would undermine scientific validity. Any necessary re-identification should remain subject to appropriate safeguards and the applicable requirements of the GDPR.

4.27. Our associations recognise that pseudonymisation is distinct from anonymisation and that pseudonymised information remains personal data where individuals are identifiable. The relevant point is that the GDPR provides a framework for protecting personal data through appropriate safeguards; it does not require organisations to anonymise information where doing so would defeat a legitimate research purpose.

Recognise professional codes of conduct and research governance

4.28. Our associations recommend that the final Guidelines give greater recognition to professional research codes of conduct, sector-specific ethical standards and self-regulatory frameworks as relevant components of an organisation's broader governance and safeguarding arrangements.

4.29. Market, opinion and social research operates within an established professional framework, including the ICC/Esomar International Code on Market, Opinion and Social Research and Data Analytics, alongside applicable national codes and professional standards.

4.30. These frameworks address confidentiality, participant protection, responsible data use and the ethical risks that may arise when research information is combined, interpreted or used in ways that could affect individuals.

4.31. Professional codes do not replace the GDPR or independently determine whether information is anonymous. They can, however, complement technical, organisational and contractual measures by establishing expectations for professional conduct, risk awareness, accountability and responsible handling of research information.

4.32. This is particularly relevant to Clause 78, Example 17, concerning employee research. The potential to infer information about individual employees from research findings raises ethical issues that are recognised within the research profession. Professional codes and established research governance arrangements provide relevant guidance on confidentiality, appropriate use and the protection of participants against harmful or inappropriate uses of research data. We therefore recommend that the EDPB explicitly reference relevant professional research codes, including the ICC/Esomar Code and applicable national codes, in Example 17 or its accompanying discussion, to illustrate their complementary role alongside technical, organisational and contractual safeguards.

4.33. Recognising these frameworks would help demonstrate that anonymisation risk management is not solely a technical exercise. It also requires professional judgement, appropriate governance and consideration of the potential consequences for individuals.

Maintain technological neutrality in relation to AI and synthetic data

4.34. We welcome the Guidelines' attention to technological developments, including AI, and agree that anonymisation assessments must remain responsive to evolving capabilities.

4.35. The final Guidelines should nevertheless remain technologically neutral and avoid unintentionally restricting legitimate research innovation involving synthetic data and AI-enabled analytical methods.

4.36. Synthetic data can support the development and testing of analytical methods, model evaluation, workflow development and data sharing where access to original individual-level records may be unnecessary. Such methods may help reduce reliance on identifiable research data in appropriate circumstances.

4.37. However, synthetic data should not automatically be presumed anonymous simply because they have been generated artificially. Their status depends on their characteristics, how they were generated, their relationship to the underlying data and the realistic possibility that they reveal or permit the identification of individuals.

4.38. Conversely, the possibility that synthetic data or AI-generated outputs could disclose information about individuals in certain circumstances should not lead to a general presumption that all such outputs constitute personal data.

4.39. The appropriate assessment should focus on the characteristics of the information and the circumstances of its use, including relevant risks of memorisation, extraction, linkage or inference where applicable.

Use neutral and technically precise terminology

4.40. We recommend reviewing the terminology used throughout the Guidelines, particularly the repeated use of the term "*violated*" when one or more criteria of the No Record Isolation, No Linkage and No Inference framework are not satisfied.

4.41. In this technical context, *"violated"* is unnecessarily strong and may imply wrongdoing or a breach of a legal obligation, when the intended meaning appears to be that a criterion has not been met in the assessment of anonymity.

- More neutral terminology would improve precision and help distinguish the outcome of a technical assessment from a finding of legal non-compliance. Depending on the grammatical context, alternatives such as "not met", "not satisfied" or "failed" would be more neutral and technically precise. This recommendation concerns descriptions of technical criteria, not references to actual breaches of legal obligations.

5. Summary of Recommendations

5.1. EFAMRO and Esomar invite the EDPB to incorporate the following changes into the final Guidelines:

- **Preserve contextual anonymisation as the legal standard**: Confirm that identifiability must be assessed in the circumstances of the relevant entity and that simplified methodologies remain optional compliance tools.
- **Clarify the treatment of aggregation:** Amend Clause 17 to recognise that aggregate data may be identifiable in some circumstances but may equally be anonymous. Clarify that aggregate research findings are not personal data merely because they inform decisions or support predictive analysis.
- **Avoid a zero-risk standard:** Reinforce the GDPR criterion of means reasonably likely to be used and distinguish realistic identification risks from hypothetical or merely conceivable scenarios.

5.2. **Apply proportionality:** Ensure that anonymisation measures and the scope and frequency of contextual reassessment reflect the actual circumstances and identification risks, while recognising the practical constraints faced by SMEs and smaller research organisations. Clarify that relevant material changes should prompt reassessment, rather than requiring continuous review of every criterion or adoption of every new technique irrespective of risk.

5.3. **Recognise legitimate longitudinal research:** Clarify that controlled re-identification, linkage over time and participant re-contact may be necessary for longitudinal and academic research, and that strong pseudonymisation may be an appropriate safeguard where full anonymisation would undermine scientific validity, subject to appropriate safeguards and applicable GDPR requirements.

5.4. **Recognise professional codes and governance:** Acknowledge the complementary role of ICC/Esomar, national research codes and professional self-regulatory frameworks alongside technical, organisational and contractual safeguards. Explicitly reference relevant codes in Clause 78, Example 17, or its accompanying discussion of employee research.

5.5. **Support responsible AI and synthetic data innovation:** Maintain a technology-neutral approach that assesses actual identifiability risks without imposing blanket assumptions about AI-generated or synthetic outputs.

5.6. **Adopt neutral terminology:** Replace *"violated"*, "violation" and related forms throughout descriptions of the three-part framework with neutral technical alternatives such as "not met", "not satisfied" or "failed", as appropriate, while distinguishing technical assessment outcomes from actual legal breaches.

6. Conclusion

6.1. Our associations welcome the EDPB's efforts to improve clarity and legal certainty regarding anonymisation in a rapidly evolving technological environment. The Guidelines provide an important opportunity to establish a more consistent understanding of identifiability and the assessment of anonymity across different processing contexts.

6.2. For the market, opinion and social research sector, it is particularly important that the final Guidelines recognise the contextual nature of anonymisation, the diversity of research methodologies and the legitimate role of aggregate statistical outputs in generating insights for business, public policy and society.

6.3. We consider that effective guidance should combine clear legal principles with proportionality, technological neutrality and practical flexibility. This would enable organisations to make reasoned, evidence-based assessments of identification risks while maintaining appropriate protection for individuals and avoiding an unattainable zero-risk standard.

6.4. The final Guidelines, therefore, should also recognise that responsible research involves a combination of technical measures, organisational controls, professional standards and appropriate governance. Where research legitimately requires continued linkage or participant re-contact, the emphasis should be on appropriate safeguards rather than an assumption that full anonymisation must always be the objective.

6.5. Ultimately, we encourage the EDPB to incorporate the recommendations set out in this response. This would strengthen the practical value of the Guidelines, improve legal certainty for organisations processing research data, particularly SMEs with limited resources, and support the continued development of trusted, high-quality and privacy-conscious research across Europe.

EFAMRO and Esomar welcome the opportunity to assist the European Data Protection Board in ensuring the Guidelines 02/2026 on Anonymisation are proportionate, fit-for-purpose, targeted and contextually appropriate. To contact us for more information:

- Kaleke Kolawole, Head of Policy: kaleke.kolawole@efamro.eu
- Federica Pizzuti, Public and Government Affairs Specialist, Federica.Pizzuti@Esomar.org