VILNIAUS STR. 31
01402 VILNIUS
LITHUANIA

T. +370 5 231 2211
E. INFO@TRINITI.LT
WWW.TRINITI.LT

E. DELIVERY BOX
ADDRESS
306233023

TRINITI
TALLINN RIGA VILNIUS

To the European Data Protection Board

REGARDING COMMENTS ON GUIDELINES 02/2026 ON ANONYMISATION

Vilnius, 2026-10-30

Following the publication by the European Data Protection Board (hereinafter referred to as the EDPB) of the Guidelines 02/2026 on Anonymisation (hereinafter referred to as the Guidelines), we would like to express our support for the EDPB's efforts to provide greater legal and practical clarity on anonymisation under the GDPR.

At the same time, based on our practical experience advising organisations of different sizes on compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the GDPR), we would like to submit the following observations and recommendations for consideration. Attention is given to the practical implementation of the Guidelines by small and medium-sized enterprises (SMEs), which often have limited legal, technical and data science resources.

1. A MORE PROPORTIONATE SME-ORIENTED APPROACH IS NEEDED

The Guidelines themselves acknowledge that the contextual approach may be complex in practice, as it requires organisations to properly identify and assess the relevant entities, their circumstances and the means reasonably likely to be used for re-identification. Where such contextual elements are difficult to establish, the Guidelines suggest that the simplified approach may be more convenient, although it may lead to a more conservative outcome. In our view, this demonstrates the need for clearer proportionality guidance for SMEs. Smaller organisations may lack the legal, technical and data science resources necessary to carry out a detailed contextual assessment in every case. We would therefore recommend introducing a simplified SME-oriented assessment tool, such as a checklist or decision tree, together with practical examples illustrating when reliance on the simplified approach would be considered sufficient.

2. ASSESSING THIRD-PARTY IDENTIFICATION CAPABILITIES AND AVAILABLE TECHNOLOGIES

The practical difficulty is particularly evident where an organisation must assess not only the recipient's own capabilities, but also whether the recipient could reasonably obtain external assistance or technology enabling re-identification. The Guidelines themselves illustrate that a technique may qualify as a means reasonably likely to be used where a recipient could easily engage a third party to perform it. For SMEs, however, it may be difficult to determine what technical capabilities, datasets or external service providers are realistically available to a recipient. We would therefore recommend clarifying the extent to which organisations may rely on recipients' representations, standardised questionnaires and contractual safeguards, particularly in lower-risk scenarios, and how far they are expected to investigate external or commercially available re-identification capabilities.

3. THE SCOPE OF EXTERNAL DATASET SEARCHES SHOULD BE CLEARER

The No Linkage criterion requires organisations to assess whether anonymised information may be linked with external datasets. For example, a small online retailer anonymising purchase histories cannot realistically investigate every website, social media platform, commercial database or other source where customers may have published related information. The Guidelines should therefore clarify the reasonable

scope of such investigations. In our view, organisations should be able to focus on external sources that are readily accessible, reasonably foreseeable and commonly used in the relevant context, rather than being expected to investigate all theoretically available information.

4. ASSESSING LAWFUL AND UNLAWFUL IDENTIFICATION METHODS MAY BE PARTICULARLY DIFFICULT FOR SMES

The Guidelines also require consideration of both lawful and potentially unlawful means of identification. For SMEs, assessing whether a third party could obtain additional information through particular legal procedures, or whether unlawful re-identification methods are reasonably likely to be used, may require complex legal, technical and economic analysis. We recommend providing clearer criteria and practical examples for this assessment, including whether organisations may rely on publicly available information, known security incidents, documented vulnerabilities and other objectively available indicators.

5. CLEARER EXPECTATIONS REGARDING TECHNICAL TESTING ARE NEEDED

Assessing whether anonymisation remains effective may require consideration of sophisticated identification methods, including advanced analytics and AI-based techniques. It is unclear, however, to what extent organisations are expected to actively test datasets against such methods. For many SMEs, adversarial re-identification testing or specialist technical validation may create disproportionate costs. The EDPB could therefore clarify when a documented assessment is sufficient and when active technical testing is expected, taking into account the sensitivity, complexity, scale and intended use or disclosure of the dataset.

6. ONGOING REASSESSMENT SHOULD FOLLOW A RISK-BASED APPROACH

The Guidelines correctly recognise that technological developments and new data sources may increase re-identification risks over time; however, continuous monitoring and repeated reassessment could create a considerable administrative and financial burden for SMEs. We recommend clarifying that reassessment may follow a proportionate and risk-based approach. For example, reassessment could be triggered by material changes such as the availability of a relevant external dataset, significant technological developments, changes in recipients or purposes, or evidence of a new re-identification technique. A continuous or fixed-frequency reassessment requirement should not be implied where the underlying context and risk remain stable.

7. MORE GUIDANCE IS NEEDED ON BALANCING ANONYMISATION AND DATA UTILITY

In practice, organisations must balance reducing re-identification risk with preserving sufficient analytical or commercial value of the data. Excessive generalisation, aggregation or perturbation may render a dataset unusable. Additional practical examples would therefore be useful, particularly for common SME use cases such as customer analytics, workforce statistics, market research or sharing aggregated data with business partners.

8. A STANDARDISED DOCUMENTATION TEMPLATE WOULD SIGNIFICANTLY ASSIST SMES

The Guidelines require organisations to document a potentially complex assessment involving the relevant entities, available means of identification, applicable perspective and the No Record Isolation, No Linkage and No Inference criteria. We would recommend that the EDPB provide a standardised anonymisation assessment template containing, at minimum, the purpose of anonymisation, relevant entities, dataset characteristics, reasonably likely means of identification, assessment against the relevant criteria, residual risks, safeguards and reassessment triggers. Such a tool would promote consistency and accountability while significantly reducing the practical burden for SMEs.

9. USE OF EXTERNAL EXPERTISE SHOULD REMAIN PROPORTIONATE

The Guidelines should also make clear that external legal, statistical or cybersecurity expertise is not necessarily required for every anonymisation exercise. The need for specialist involvement should depend on factors such as the sensitivity, complexity and dimensionality of the dataset, the recipients involved and the intended form of dissemination. Otherwise, there is a risk that SMEs may perceive anonymisation as practically inaccessible without significant external expenditure.

10. MORE SME-SPECIFIC PRACTICAL EXAMPLES WOULD BE USEFUL

Finally, we would encourage the EDPB to include examples reflecting typical SME environments, such as a small retailer analysing purchasing trends, a professional services firm producing client statistics, a small employer analysing workforce data or a small healthcare provider preparing aggregated statistics.

OVERALL RECOMMENDATION

The Guidelines provide valuable legal and technical clarification and establish a useful framework for assessing anonymisation, however, without additional proportionality guidance, there is a risk that their practical application may become excessively complex and resource-intensive for SMEs. We would therefore encourage the EDPB to retain the substantive standard of anonymisation while introducing clearer proportionality principles, simplified assessment tools, defined limits on external investigations and more practical SME-specific examples.

Best regards,

APB TRINITI

Lithuania