DMA Finland's (ASML) comments on EDPB Guidelines 02/2026 on Anonymisation

SUMMARY

Assessments and analyses carried out by companies within the framework of the GDPR, relevant case law and EDPB guidance should enable controllers to reach conclusions on which both controllers and processors can reasonably rely.

EDPB guidance should not introduce a degree of relativism into controllers' assessments of anonymity that makes those assessments unworkable in practice.

- Several subsequent parts of the draft Guidelines appear difficult to reconcile with that starting point in paragraphs 7-12 which recognises that the assessment of whether information constitutes personal data is contextual.
- The mere fact that the possibility of identification cannot be ruled out is not sufficient for data to cease to qualify as anonymous.
- The assessment of the means reasonably likely to be used should not take purely theoretical or speculative possibilities into account.
- A means of identification should be considered where its availability and use are realistically foreseeable, considering all objective circumstances.
- Unlawful conduct should be considered only where the specific circumstances provide sufficient grounds for considering such conduct reasonably likely.

EU seeks to strengthen its competitiveness, foster innovation and simplify regulation. Anonymisation should support these goals by enabling responsible data use while ensuring s trong data protection and legal certainty.

1. Theoretical possibility should not replace the contextual threshold of reasonable likelihood (paragraph 17)

Draft Guidelines correctly state in paragraph 8 that identifiability is a question of likelihood rather than an absolute possibility. Paragraph 18 states that personal data requires an

identified or identifiable individual using means reasonably likely to be used. Paragraph 17 does not fully reflect this limiting principle when stating that aggregate data may relate to an individual where a technique **"**could be used" to reveal information relating to that individual. The existence of a technically conceivable transformation of aggregate data is not necessarily sufficient to establish that the aggregate information itself relates to an individual. Draft Guidelines in paragraphs 69-70 recognise that personal information may be inferred from anonymous data without thereby making the source data personal. Paragraph 17 should clearly clarify that the mere theoretical availability of a technique is insufficient. There should be a concrete connection between the given data and the individual.

Hypothetical data breaches or unlawful access by third parties should not automatically prevent data from qualifying as anonymous unless concrete circumstances make such ident ification scenarios reasonably foreseeable. EDPB should fully follow the risk-based approach established by the CJEU and GDPR.

2. "Cannot be ruled out" vs "means reasonably likely to be used" (paragraph 21)

According to the paragraph 21, data should be treated as personal where *"it is reasonably likely that an entity can transfer the data to a third party; and it "cannot be ruled out" that the recipient has means to identify the individual"*. This is a materially different threshold from the one set by the draft Guidelines themselves in paragraphs 8, 20, 22, 28 and 29, which focus on actual likelihood and on means reasonably likely to be used. Rather than requiring a positive basis for concluding that identification is reasonably likely, "cannot be ruled out" may require the entity to exclude different kind of hypothetical identification possibilities. A theoretical recipient with hypothetical additional information should not be sufficient. "Cannot be ruled out" test should be replaced with a positive reasonable-likelihood test.

3. Identifiers, uniqueness and singling out should not automatically amount to identification of a natural person (paragraphs 23-25, examples 5 and 6)

Paragraph 23 lists a name, IP address, social security number and email address together as examples of single pieces of unique data that may identify an individual. And paragraph 25

then states that a MAC address can identify a device *"and, in turn, the individual using the device"*. An IP address, device identifier or data pieces mentioned may distinguish a connection, device or browser. That does not necessarily establish that the natural person behind it is identifiable. The fact that one person on a street is the only person simultaneously wearing a black suit and walking a dog establishes uniqueness within the observed context in example 5. The Guidelines then state that this description *"allows for them to be identified"*. That conclusion moves too quickly. Example 6 makes a similar move from uniqueness to identification in relation to device fingerprinting.

Recital 26 of GDPR treats singling out as a means that may contribute to identification but it should not automatically become an independent definition of identification. Paragraph 99 recognise this accepting that records may be unique while the data nevertheless remains anonymous where the attributes cannot reasonably be linked back to individuals. Examples 5 and 6 should distinguish between uniqueness > singling out > identifiability of a natural person.

4. Treatment of unlawful actors and hypothetical future breaches should be made internally consistent (paragraphs 30-33, 88-90 and example 22)

Paragraph 30 includes among potentially relevant entities rogue employees, domestic and foreign intelligence agencies, unethical companies and cybercriminals. This could lead to an almost unlimited identifiability assessment. Paragraphs 32–33 provide a significantly more defensible limiting principle. Paragraph 89 similarly states that where appropriate security controls exist, access constitutes a means reasonably likely to be used only by authorised users and not unauthorised actors.

Example 22 is very problematic. Despite "*strong state-of-the-art cybersecurity measures",* the research institute considers a future leak, human error and hacking sufficiently possible that hackers and accidental recipients are treated as relevant entities. This example appears substantially more precautionary than paragraphs 33 and 89. The Guidelines should state explicitly that unlawful access must not be included merely because it is conceivable. It should only be included where concrete circumstances make that unlawful access

reasonably foreseeable, consistently with paragraph 33. A hypothetical future data breach should not cause currently anonymous information to be treated as personal data before the breach has occurred.

5. Motivation should remain an objective factor in the ex ante assessment (paragraphs 31 and 83)

Paragraph 31 cautions against relying on lack of motivation and refers to identification occurring accidentally or through negligence. Paragraph 83 similarly states that re-identification techniques may be used intentionally or unintentionally. An unforeseeable accident cannot automatically establish ex ante that identification was reasonably likely. Paragraph 31 should state that subjective intention is not determinative, but objective indications of motivation, incentives, expected behaviour and purpose of use remain relevant when assessing whether a means is reasonably likely to be used.

6. Contractual restrictions should not be categorically limited to a supporting role (paragraph 34)

Paragraph 34 states that a contractual prohibition should not be treated as a prohibition by law and that contractual measures "*should only be used to complement technical measures*". The relevant legal test described elsewhere in the draft Guidelines is whether identification is reasonably likely in practice, taking account of all objective factors. There is no evident reason within that test to impose a categorical rule that an effective contractual arrangement can only ever "complement" a technical measure.

Paragraph 34 should focus on effectiveness rather than the formal category of the safeguard. *"Should only be used to complement technical measures"* should be replaced with statement that contractual measures should be assessed according to their actual reliability, enforceability and effectiveness, alone and in combination with other safeguards.

7. A single identifiable record should not automatically determine the legal status of objectively separable anonymous records paragraph 36)

Paragraph 36 provides that a dataset as a whole should only be considered anonymous where re-identification risk is insignificant for all included individuals. If a dataset contains both personal and anonymous data and the different parts are not "treated separately", the whole dataset should be treated as containing personal data. The footnote relies by analogy on the Meta v Bundeskartellamt treatment of datasets combining special-category and ordinary personal data. This analogy should be reconsidered. There is a fundamental difference between ordinary personal data and special-category personal data, compared to personal data and information which does not constitute personal data at all. The former categories are both within the GDPR, the latter are not.

Paragraph 87 reinforces the concern by stating that a re-identification technique may be successful even where it succeeds against only a single individual in a larger dataset. That can establish that the relevant record is personal data. It does not automatically establish that objectively distinguishable records relating to other individuals are also personal data. Paragraph 36 should distinguish between whether a dataset contains personal data at all; and which identifiable or objectively separable parts of that dataset fall within the GDPR. The relevant question should be whether the anonymous and personal parts are objectively separable or distinguishable, rather than whether the controller happens to "treat" them separately.

8. Documentation should not become a condition for proving that the GDPR does not apply (paragraphs 41,47)

Paragraph 41 recommends documentation of the anonymisation process and states that the documentation should be retained after anonymisation has been completed. Documenting the assessment should be encouraged. However, the Guidelines should make clear that documentation is evidence supporting the assessment, not a constitutive requirement for anonymity.

Whether the GDPR applies must ultimately depend on whether information is personal data, not on whether an entity has produced a particular dossier demonstrating that it is not. The issue becomes particularly important in paragraph 47, which describes a risk of a "false positive" anonymity finding where the assessor is unaware of an entity possessing means reasonably likely to be used for identification. An entity cannot reasonably be expected to disprove unidentified means possessed by unidentified entities. The proper test should be based on the entities, information and means reasonably foreseeable on the basis of objective circumstances at the time of assessment.

9. Future developments should only count where they are reasonably foreseeable, not merely imaginable (paragraphs 88–93)

Paragraph 29(e) correctly states that reasonably foreseeable technological developments are relevant. Paragraphs 88-93 should consistently retain that limitation. Paragraph 88 recommends safety margins to address evolving capabilities, while paragraphs 92-93 suggest that AI and agentic AI are likely to reduce the cost of re-identification and gathering information from multiple sources. There is nothing objectionable in requiring an assessment to take reasonably foreseeable technological change into account. The difficulty arises if the possibility of unspecified future technical advances is used to keep information within the GDPR indefinitely. Final Guidelines should expressly cross-reference paragraph 29(e) and state that only technological developments that are reasonably foreseeable within the relevant period and processing context should affect the present classification of the data.

Effective anonymisation reduces data protection risks and enables responsible data use. Guidelines should therefore encourage investment in anonymisation by providing clear, predictable criteria that support consistent assessments across the EU and avoid unnecessary uncertainty for future innovation.