IPMPC
International Pharmaceutical & Medical Device Privacy Consortium

30 October 2026

IPMPC Response to the European Data Protection Board's Public Consultation on Guidelines 02/2026 on Anonymisation

The International Pharmaceutical and Medical Device Privacy Consortium (IPMPC) appreciates the opportunity to comment on the European Data Protection Board (EDPB) Guidelines 02/2026 on Anonymisation (hereinafter, 'the Guidelines'). The IPMPC supports the EDPB's efforts to promote clarity and consistent application of data protection requirements across the EU.

The IPMPC is a global privacy and digital policy organisation focused on the concerns of the pharmaceutical and medical device industries. With over 45 member companies and hundreds of member participants from around the world, the IPMPC strives to advance members' compliance with privacy, security, AI, and other digital governance obligations, with the ultimate aim of supporting innovation in health diagnostics, treatments, and disease prevention, and enabling the delivery of life-saving and quality-enhancing healthcare to patients. For 25 years, the IPMPC has actively engaged with policy makers and data protection authorities across Europe to facilitate regulators' understanding of why and how data is processed in the pharmaceutical and medical device industries and to promote policies that align regulatory goals with members' data needs.

The medical technology and pharmaceutical industries share a long history of and commitment to advancing medical science. By turning scientific research into solutions for patients, healthcare professionals, and health systems, the medtech and pharmaceutical industries have contributed to better outcomes for patients and greater efficiency in healthcare.

A. The Concept of 'Identifiability'

1. Contextual Analysis

The IPMPC agrees with the EDPB that whether information constitutes personal data requires a contextual analysis of the capabilities of those who might identify the data subject. Each entity's perspective should be considered since a particular set of information may be personal data as to one entity but anonymous as to another. This is a necessary conclusion of the Court of Justice's judgment in *EDPS v SRB* (C-413/23).

The IPMPC also welcomes the Guidelines' recognition that information does not become personal data merely because it relates to a natural person; rather, the person must also be identified or identifiable using means reasonably likely to be used. This distinction is

particularly important for scientific research and analytics, where a dataset may support learning about a population while keeping individuals unidentified and unidentifiable. Likewise, the likelihood of successful identification need not be zero; it should be insignificant in reality when assessed from the relevant perspective.

The contextual principle should remain the organising principle throughout the Guidelines, including the legal analysis, technical criteria, and examples. The Guidelines should not directly or indirectly favour an approach that requires consideration of hypothetical recipients, unknown capabilities, or speculative future attacks. Instead, the final text should make clear that anonymity is *de jure* assessed from the perspective of the relevant entity and by reference to that entity's reasonable capabilities and access to identifying information.

2. Identifiability Must Be More Than Uniqueness

The Guidelines should state clearly that uniqueness, singling out, or record isolation does not by itself identify a natural person. A unique combination of attributes must be realistically matchable to a real individual through means reasonably likely to be used. Record isolation should be treated as a screening criterion, not a conclusion, and the qualification in paragraphs 98-100 should be applied consistently throughout the Guidelines. The analysis should also distinguish stable quasi-identifiers from transient physiological, behavioural, or cognitive measurements whose values change over time and may not support reliable matching.

B. Assessment of Means Reasonably Likely to Be Used to Identify an Individual

1. Relevant Factors to Be Considered

The Guidelines should provide a structured and evidence-based proportionality test for determining which means are reasonably likely to be used to identify an individual. Relevant factors should include the number and type of capable actors; realistic access to the dataset and auxiliary information; technical capability; time, cost, and labour; likely benefit; legal and contractual consequences; the availability of easier alternative routes to the same information; temporal change in data values; and the probability and consequences of successful identification.

The Guidelines should avoid dismissing motivation as a factor, since it is relevant in assessing likely re-identification risks. Testing the effectiveness of anonymisation techniques and controls against an individual motivated to attempt re-identification helps assess whether re-identification is highly unlikely in practice. Likewise, foreseeable technological developments should be assessed using scientifically grounded evidence, not speculation about any technique that might some day exist or be inexpensive to run. Theoretical future capabilities, including generic predictions about AI, should not make data presently identifiable without sufficiently

concrete evidence, and any need to revisit an assessment should be tied to proportionate review triggers.

2. Technical, Organisational, Contractual, and Legal Controls

The Guidelines provide examples of things which would stop means from being reasonably likely to be used by a particular entity to identify an individual. In particular, the Guidelines note that 'means may not be reasonably likely to be used if the likelihood of identification appears, in reality, to be insignificant because it would be impossible to do; because it would involve disproportionate effort in terms of time, cost and labour; or because of a legal prohibition.' With respect to contractual restrictions, the Guidelines state:

> A prohibition set out in a contract (even if it is legally binding upon its parties) should not be treated as a prohibition by law. While contractual terms may have an effect on the means reasonably likely to be used, they should only be used to complement technical measures and it is important to carefully consider the actual strength of their effect. Among other things, the measures should be reliable, verifiable and enforceable, bearing in mind that contractual measures can typically be subject to revision, or may even be disregarded entirely by the parties.

Contractual terms can play a significant role, along with other technical and organisational measures, in ensuring that a dataset cannot be re-identified. The IPMPC agrees that a contractual prohibition is not equivalent to a statutory prohibition and that contractual wording alone does not establish anonymity. However, this should not result in effective contractual safeguards being given only marginal weight, nor should the possibility that a contract could be amended or breached cause its safeguards to be disregarded without assessing how likely that event is. Indeed, contractual safeguards play an important role in the GDPR both under Article 28(3) (processor contracts) and Article 46(2)(c) (standard contractual clauses for international transfers), and they can be equally important in the context of anonymisation by prohibiting attempts at re-identification, restricting uses and disclosures, and requiring that a dataset is handled confidentially and securely. The IPMPC therefore recommends that the EDPB amend the above quoted section of the Guidelines to focus on the reliability, enforceability, and practical operation of contractual safeguards and on how they can be most effectively implemented as a safeguard against re-identification. Where a safeguard is considered insufficient, the Guidelines should explain why in the particular factual setting, rather than implying that contractual measures have inherently limited value.

The final Guidelines should similarly recognise that enforceable organisational measures, confidentiality obligations (including professional and clinical confidentiality), internal policies, access controls, encryption, and controlled research environments can

materially affect which means are reasonably likely to be used. Combined technical, organisational, contractual, legal, and professional-confidentiality safeguards should be given meaningful weight. Relevant factors include enforceable re-identification prohibitions, audit rights, access restrictions, onward-transfer controls, security controls, and evidence of their practical effectiveness. The weight given to these measures should turn on their reliability, verifiability, enforceability, and practical operation, and verification should remain proportionate to risk rather than requiring routine audits in every case. For consistency with Articles 24, 25, and 32 GDPR, which require controllers to implement appropriate technical and organisational measures, the Guidelines should confirm that such measures support anonymisation conclusions rather than raising questions as to their sufficiency.

For example, the Guidelines should specify that the 'No Linkage' criterion may be satisfied if the relevant entity cannot realistically access and combine additional information because of effective technical, organisational, or contractual controls, even where attributes could theoretically be linked to another dataset. The theoretical existence of another dataset should not determine the outcome by itself.

The Guidelines should distinguish authorised access from credible unlawful access and should not treat the mere possibility that a party could disregard the law, a contract, or security controls as sufficient to defeat anonymity. Rogue-employee, malicious-actor, interception, or state-access scenarios should be included only where a concrete and proportionate assessment shows that such means are realistically likely to be used. Concrete evidence of a realistic breach or misuse scenario may be relevant. However, the Guidelines should distinguish the personal-data question from the security-of-processing question: an inability to guarantee that a breach or other unlawful access event will never occur should not by itself defeat anonymity or reintroduce a zero-risk standard.

B. The Need for Practical, Clear Guidance

Consistent with the contextual approach described above, the IPMPC supports practical guidance and recommends that the EDPB streamline the number of tests, standards, and sub-tests proposed to reduce complexity. To facilitate consistent application of the framework, the EDPB should provide a consolidated roadmap or decision tree that maps the legal and technical analyses and explains how they interact. In particular, the separate 'content, purpose, effect' test for whether information 'relates' to an individual should be integrated into that roadmap so that it does not create an additional, disconnected analytical layer.

The Guidelines can be made more useful if each example that illustrates unsuccessful anonymisation also identifies a solution and safeguards to resolve risks and achieve anonymisation.

The following modifications and additions to the Guidelines would be of particular value to the scientific research community:

1. *Mixed Datasets, Rare Records, and Quantitative Evidence*

The Guidelines should explain how to handle datasets containing rare or unique records without automatically treating the entire dataset as personal or requiring removal of clinically important information. Proportionate options may include targeted suppression, generalisation, access restrictions, output checking, or separate processing. Established statistical disclosure-control methods, including risk-based anonymisation and k-anonymity, should be recognised as relevant evidence within the contextual legal assessment. Non-binding examples or benchmarks would improve consistency without creating an inflexible safe harbour.

2. *Controlled Access and Public Release*

The Guidelines should distinguish public release from controlled access by approved researchers in restricted environments. The assessment should consider the actual capabilities and access of authorised users and the effectiveness of technical and organisational controls, rather than assuming that human error, leakage, or cyberattack will necessarily defeat state-of-the-art safeguards.

3. *Aggregate Data, Linkage, and Reference Populations*

Aggregate information should be treated as relating to an individual only where a realistic technique can derive meaningful information about an identified or identifiable person. The Guidelines should distinguish theoretical de-aggregation from realistic reconstruction or inference, and reconcile the treatment of aggregates across the text. Linkage analysis should be bounded by the relevant reference population, equivalence classes, population size, attribute resolution, the availability and reliability of exact matching data, and the perspectives of entities that can realistically access both datasets.

C. Reusable Assessments and Proportionate Reassessment

Organisations should be able to use validated standard assessment frameworks, documented reasoning, data classes, and repeatable controls for recurring categories of data and processing, with dataset-specific checks for material differences. Reassessment should be linked to defined triggers, such as material changes in access, auxiliary data, intended use, known incidents, or available identification techniques. A wholly bespoke assessment for every similar clinical or research dataset, or indefinite reassessment based on speculative technical progress, would create disproportionate burden and impede responsible secondary use of health data, research, and innovation.

D. Disclosures Among Related Entities, Processors, and Internal Functions

The Guidelines acknowledge that whether information is personal for a particular entity should typically be referenced to that entity's own perspective. The GDPR treats each legal entity as a separate entity, even if the entities are part of the same corporate family, with the result that information that is personal data as to one corporate affiliate may be anonymous as to another. The fact that two legal entities are part of the same corporate family may be relevant to whether an entity has means reasonably likely to be used to identify the subject(s) of a dataset, but it is not determinative. The same overall anonymisation analysis applies, although the impact of common ownership or control, shared IT infrastructure, and similar factors must be considered. The IPMPC suggests that the EDPB directly address such scenarios in the Guidelines.

The IPMPC also encourages the EDPB to reconsider its position that once information is personal data as to a particular function within a legal entity, all functions and departments within that legal entity must similarly treat the information as personal data. This position does not meaningfully protect individuals' privacy interests. Internal technical and organisational separation, access limitations, and governance controls can effectively limit which functions and departments possess the means to identify data subjects. The EDPB should encourage the implementation of such internal, privacy-enhancing controls and describe in the Guidelines how such controls can sufficiently minimise identification risks.

The Guidelines should likewise address processors and longer processing chains. Data should not automatically be treated as personal for a recipient merely because another entity, affiliate, controller, or function retains identifying information. The assessment should instead examine credible onward-access routes, effective separation, contractual restrictions, shared infrastructure, and whether the recipient has realistic means reasonably likely to be used to identify an individual.

E. Lawfulness of the Anonymisation Process

The Guidelines note that 'anonymisation must have a legal basis under Article 6 GDPR, and that one of the exemptions under Article 9(2) GDPR should apply if the dataset contains special category personal data'. There are several legal bases that controllers can potentially rely upon under Article 6 for such processing, including legitimate interests. When a controller wishes to anonymise personal health data for scientific research purposes, the relevant Article 9(2) condition can be found in Article 9(2)(j) GDPR.

Article 9(2)(j) GDPR permits processing of personal health data where such processing is necessary for scientific research purposes in accordance with Article 89(1), 'based on EU or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the

fundamental rights and the interests of the data subject.' In the context of anonymising personal health data for scientific research purposes, Article 89(1) GDPR itself serves as the EU law referenced in this phrase. Specifically, Article 89(1) requires controllers to anonymise data for scientific research purposes wherever those purposes can be fulfilled in that manner ('Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.'). The IPMPC encourages the EDPB to expressly affirm this interpretation.

Relatedly, the IPMPC encourages the EDPB to affirm that anonymisation and pseudonymisation undertaken as protective operations in connection with lawful processing for the same or compatible purposes are not to be treated as new and independent purposes requiring a separate Article 6 legal basis or Article 9(2) condition. Anonymisation may itself further compliance with data minimisation, storage limitation, and data protection by design.

A scientific research example in the Guidelines would help illustrate these points. The example should explain how the stated requirement for a legal basis for anonymisation interacts with Article 89(1) GDPR, and how further processing for scientific research purposes relates to the original purpose of collection, given that Article 5(1)(b) GDPR provides that such further processing is not to be considered incompatible with the initial purposes. The Guidelines should avoid an interpretation under which researchers face greater legal uncertainty when anonymising data than when continuing to process it in identifiable form.

The final Guidelines should also distinguish the anonymisation operation from the subsequent use of the resulting information. Once information is genuinely anonymous, its subsequent use falls outside the GDPR and need not be for the same processing activity as the original purpose. If the data remains personal or pseudonymised, the lawfulness of that subsequent processing must be assessed separately under the GDPR. More broadly, the Guidelines should explain how Articles 6, 9(2)(j), and 89 apply to the preparation of health data for secondary research and should avoid interpretations that incentivise unnecessary recollection of data or additional medical interventions where existing data can responsibly be reused.

We appreciate the opportunity to provide comments on the Guidelines. Please do not hesitate to reach out to us should any of our comments require further clarification.