efpia
European Federation of Pharmaceutical Industries and Associations



EFPIA response to the public consultation on EDPB Guidelines 02/2026 on anonymisation

Date: 27/10/2026 ● **Version:** **Final**

Introduction

EFPIA welcomes the opportunity to comment on the European Data Protection Board's draft Guidelines 2/2026 on Anonymisation.

A clear and workable interpretation of anonymisation is essential to protect individuals while enabling responsible health-data use for scientific research and medicines development.

EFPIA welcomes the recognition that information may be anonymous for some entities but not others, that the likelihood of identification need not be zero, and that anonymisation does not necessarily require deletion of the original data. We particularly support the distinction between information that merely relates to a natural person and information that identifies or makes that person identifiable. This distinction is essential for anonymised research datasets that retain analytical value concerning individuals or populations without permitting those individuals to be identified using means reasonably likely to be used We also support the distinction between record isolation and identification, and the recognition that failure of an individual technical criterion does not automatically establish that data are personal.

An effective anonymisation assessment should consider data transformation together with the technical, organisational and legal safeguards governing access and use. These measures should deliver effective protection while preserving the information needed for scientifically valid research.

Our principal concern is ensuring that the technical framework and examples consistently reflect the Guidelines' contextual legal approach. Requirements to consider hypothetical recipients, unknown capabilities or speculative future attacks should not, in practice, reintroduce an absolute standard that the Guidelines expressly reject.

Given the number of interacting legal and technical tests—including the "content, purpose and effect" test, the relevant perspective, record isolation, linkage, inference and the assessment of means reasonably likely to be used—EFPIA recommends that the final Guidelines xpand the flowchart in Annex 1 into a consolidated roadmap or decision tree covering both aggregate and

record-level data. This should explain the sequence of the analysis, the evidence expected at each stage and how the individual criteria interact. Worked examples, including examples from controlled health-research environments, should accompany that roadmap and illustrate when aggregate outputs may support reconstruction, linkage or specific and meaningful inference concerning an individual.

The Guidelines should also explain how their assessment framework relates to recognised de-identification frameworks, particularly regarding assessment of the data environment, auxiliary information realistically available to a potential adversary, and the resulting risks of linkage or inference. Such frameworks may support the assessment without replacing the applicable legal standard under the GDPR.

We encourage the EDPB to include further examples addressing controlled pharmaceutical research, clinical-trial data and the implementation of the European Health Data Space. Sectoral initiatives, including the EFPIA GDPR Code of Conduct, could help inform this work.

Preserve the contextual approach throughout the Guidelines

EFPIA supports the recognition that anonymity depends on the applicable perspective and that an insignificant likelihood of identification can satisfy the legal standard.

We particularly welcome the clarification that the voluntary simplified approach is voluntary, and it is not the only means to demonstrate anonymity. Controllers may rely directly on a properly documented contextual assessment. Failiure to satisfy the simplified approach does not establish that the information remains personal data.

However, describing that approach as providing greater confidence could encourage organisations or authorities to treat it as the preferred benchmark. In research settings, this could lead to unnecessary transformation or withholding of data.

We would welcome a further clarification that a documented contextual assessment is sufficient, and that Guidance, certification or supervisory practice should not make the simplified approach a *de facto* requirement.

Clarify when onward transfers affect identifiability

EFPIA recognises that identification can involve several entities and that credible onward-transfer scenarios must be assessed.

Nevertheless, the Guidelines refer to circumstances where it "cannot be ruled out" that a receiving entity possesses identification means. This wording risks replacing an objective likelihood assessment with a requirement to disprove unknown possibilities.

The assessment should address the likelihood of the complete identification pathway, including access to the given data, access to additional information and the ability to combine them effectively. A theoretical possibility of access should not be sufficient: the relevant entity must have, or be reasonably likely to obtain, meaningful access to the data and additional information needed to complete the identification pathway. Where identification would depend on multiple transfers or entities, the likelihood of the complete chain should be assessed rather than treating each theoretically possible step in isolation.

EFPIA therefore recommends requiring objective evidence that the recipient possesses, or it is likely to obtain, means capable of identification. Hypothethical uncertainty about the capabilities of the recipient should not, without evidence, be sufficient to conclude that data are personal for that recipient.

Distinguish research roles and the relevant perspectives

EFPIA recognises that identifiability should be assessed separately from the perspective of each relevant entity. Where the originating controller possesses means likely to be used for identifying individuals, processing remains subject to GDPR. This should not determine whether data are anonymous for an independent recipient.

The Guidelines would benefit from more detailed treatment of research arrangements. In the context of pharmaceutical industry different subjects may perform different functions. Their roles cannot be inferred solely from the fact that data originate in the same study.

EFPIA recommends adding further examples distinguishing processing on a sponsor's behalf from primary public disclosure under regulatory transparency and from independent secondary research as these setting involve differrent actors, access conditions, risks and controls. The examples should explain whether and how the return of aggregate research findings, scientific collaboration or study funding affects the assessment.

The Guidelines should also clarify whether, and under what conditions, information may be anonymous from the perspective of a particular function or department within a legal entity. Relevant considerations could include effective functional separation, role-based access controls, segregation of duties, documented governance and the absence of meaningful access by that function to identifying information. Any such approach should preserve the controller's accountability for ensuring that the separation is effective in practice.

Give effective contractual and organisational controls appropriate weight

EFPIA welcomes the recognition that access restrictions and technical, organisational and contractual measures can affect the means reasonably likely to be used.

We agree that a contractual prohibition is not equivalent to a statutory prohibition, but it may nevertheless create legally binding and enforceable obligations, with meaningful consequences for breach. that Contractual wording alone does not establish anonymity. However, this should not result in effective contractual safeguards being given only marginal weight.

EFPIA encourages the EDPB to clarify that enforceable contractual and organisational measures can materially affect the outcome of a contextual assessment. Where contractual measures are supported by role-based access controls, segregation of duties, audit rights, monitoring, sanctions and technical restrictions, they alter the practical capability and incentive to obtain or use additional information. These measures should therefore form part of the objective evidence used to determine whether a particular means is reasonably likely to be used. Their weight should not depend on a predetermined minimum level of data transformation.

Consistently with the contextual approach, the Guidelines should distinguish between publicly available information and information held in a controlled environment. Publicly available data may be accessible to a broad range of actors, whereas data subject to effective technical, organisational and contractual restrictions should ordinarily be assessed from the perspective of authorised users, unless objective evidence demonstrates a concrete and reasonably likely route of unauthorised access.

Align hypothetical breach scenarios with the contextual standard

EFPIA agrees that credible risks of unlawful access must be considered. We welcome the reference to evidence of a concrete risk and the recognition that appropriate security controls can exclude unauthorised actors from reasonably likely access.

We recommend to further clarify that the inability to guarantee that a breach will never occur should not defeat anonymity. A motivated-intruder analysis may provide a useful operational benchmark, but it should not be displaced by speculative capabilities or remote possibilities of unlawful conduct. Unauthorised access should affect the anonymisation assessment where objective evidence demonstrates a concrete and reasonably likely identification pathway; otherwise, the risk should principally be addressed through the GDPR's security and personal-data-breach requirements.

Clarify the legal basis for anonymisation as a protective operation

EFPIA welcomes the presumption that the legal basis and Article 9 condition coincide with those applicable to the preceding processing where anonymisation forms part of the same processing activity and pursues the same or compatible purposes.

However, limiting this presumption to identical purposes may create uncertainty where anonymisation is undertaken to enable compatible further processing for scientific research.

EFPIA considers that anonymisation and pseudonymisation, when undertaken as protective operations in connection with lawful processing, should not be treated as independent purposes requiring a separate legal basis or Article 9 condition. Anonymisation may also contribute to compliance with the principles of data minimisation and storage limitation and with the obligation of data protection by design.

EFPIA recommends that the Guidelines distinguish the anonymisation operation from the subsequent use of the resulting information. They should clarify that anonymisation undertaken as a safeguard within lawful processing for the same or compatible purposes does not require an additional legal basis solely because the resulting information is intended for subsequent use. Once information is genuinely anonymous, its subsequent use falls outside the GDPR. Where the

information remains personal or pseudonymised, the lawfulness of the subsequent processing must be assessed separately under the GDPR.

Provide workable guidance on linkage and inference

EFPIA supports the recognition that linkage does not invariably establish identification and that general population-level knowledge should be distinguished from specific and meaningful inference about an identifiable person.

These distinctions are particularly important for research intended to generate generalisable knowledge. EFPIA therefore recommends providing examples related to such kind of research.

The linkage criterion should be assessed in its specific context, including whether the relevant entity can realistically access and combine the additional information required for linkage. The theoretical existence of another linkable dataset should not, by itself, determine the outcome where effective technical, organisational or contractual controls make access to that information not reasonably likely. Accordingly, access controls, encryption, contractual restrictions and governance measures may materially affect whether linkage constitutes a means reasonably likely to be used, even though those measures do not replace the technical assessment.

Where a particular record creates a materially higher identification risk, the Guidelines should clarify whether that record or a separable portion of the dataset may be addressed through targeted measures, such as suppression, generalisation, access restrictions or separate processing. Identification of one record should not automatically determine the status of the remaining data where the relevant portion can be effectively separated and does not materially increase the identifiability of other individuals.

Make reassessment and safety margins proportionate

EFPIA welcomes the clarification that the Guidelines do not automatically require reassessment of previously assessed datasets. We also support reassessment where material changes affect the original conclusion.

Reassessment should be proportionate and triggered by material changes capable of affecting the original conclusion, rather than by a fixed periodic review cycle or continuous monitoring obligation.

Organisations should be able to reuse validated assessment methodologies, documented reasoning and control frameworks for materially similar recurring datasets or processing operations. Proportionate checks should nevertheless confirm that the relevant assumptions

remain applicable, including the population, data characteristics, intended recipients, disclosure environment and available auxiliary information.

Avoid general presumptions about the feasibility of identification attacks

EFPIA supports assessment against scientifically grounded evidence and relevant technological developments.

However, the Guidelines lack sufficient precision regarding the practical accessibility, cost and success rate of documented identification techniques. The ability to run an algorithm does not necessarily establish the ability to identify individuals successfully in a particular dataset. The assessment should be based on empirically supported, context-specific evidence, including the availability of the necessary auxiliary data, expertise and computing resources and a realistic prospect of successful identification.

EFPIA would also welcome non-binding examples of how established statistical and risk-based methods may support the contextual assessment. The Guidelines should make clear that no individual method or quantitative threshold is universally determinative and that its relevance depends on the data, reference population, disclosure environment and realistically available additional information.

Interaction with the EHDS and future EU health data framework

The Guidelines should better explain their interaction with the EHDS and support the broader EU objective of enabling responsible secondary use of health data. Anonymisation requirements should recognise the safeguards provided by controlled research environments and preserve the scientific utility of data.

EFPIA recommends a consistent approach across the GDPR, EHDS and emerging legislative frameworks, including the Digital Omnibus and Biotech Act proposals. The final Guidelines should support coherent implementation and avoid additional uncertainty or fragmentation for research conducted across Member States.

Closing recommendation

EFPIA encourages the EDPB to preserve the Guidelines' contextual legal standard and make its practical application more predictable. Sector-specific examples, proportionate documentation and recognition of effective combined safeguards would help organisations protect individuals while preserving the utility of data for research.

EFPIA would welcome further engagement with the EDPB, health authorities and research stakeholders to develop these examples, drawing on established pharmaceutical disclosure and controlled-access practices.