Questions to be raised in the public consultation on the "Guidelines 02/2026 on Anonymisation"

1. Risks of the contextual approach in the field of health research and the use of genetic data

In research, when assessing the nature of data and the applicability of data protection legislation, the entire set of processes and the connections between entities and processing operations must be taken into account. In certain processing activities, the re-identification of the data subject is an intrinsic element of the purpose of the processing, in order to ensure compliance with the legal obligations laid down in the applicable legislation.

For example, in the case of biobanks, the researcher receiving the sample cannot identify the source individual. Traceability is maintained by the biobank, together with the contact details needed to communicate findings that may be relevant to the health of the individual or their relatives. This obligation is laid down in the legislation governing research involving biological samples. This means that, although the researcher cannot identify the source individual independently, the processing operations carried out by the researcher will have an impact on that individual.

This type of data processing, particularly when genetic data are involved, requires data protection legislation to be applied at every stage, even where controllers may not be able to identify the data subjects at certain stages, since the processing operation as a whole will affect their fundamental right to control their own information. Considering the data available to the researcher as exempt from data protection legislation, and therefore allowing them to be disclosed or stored in an insecure environment, may result in a breach of the source individual's fundamental right to informational self-determination, as they may lose control over information that could directly affect their health.

In this regard, Article 11 GDPR recognises that data protection legislation remains applicable where a controller processes personal data that do not require the identification of the data subject. This would apply to the example described above, in which the researcher does not need to identify the individual, even though traceability is an essential element of the processing activity.

Paragraph 24 of the Guidelines 1/2026 acknowledges that genetic attributes may contribute to identifying an individual, particularly when combined with other data. This risk is particularly relevant in biomedical and genomic research, biobanks and studies involving rare diseases.

It would therefore be useful to clarify under what circumstances individual genetic data or health data may be considered anonymous, and how the risk of re-identification should be assessed where the recipient cannot identify the individuals concerned, but a traceability obligation exists that directly affects the possibility of re-identifying the data.

However, as stated above, legal protection should not depend solely on identifiability at each individual stage, but also on the foreseeable effects of the processing activity as a whole. Assessing each stage separately may result in the same data being assigned different legal classifications and may overlook the connections between the different stages of the process.

2. Controller liability in the event of a false positive

The Guidelines acknowledge that the contextual approach may give rise to false positives where data are deemed anonymous without all reasonably likely means of re-identification having been identified (paragraph 47). Likewise, paragraph 35 establishes that data previously considered anonymous must be treated as personal data again if the risk of identification ceases to be negligible.

In order to strengthen legal certainty, it would be advisable to clarify how controllers should act when an anonymisation assessment ceases to be valid, distinguishing between an assessment that was initially reasonable and identification that subsequently becomes possible as a result of technological advances, such as artificial intelligence.

What obligations must a controller fulfil when it discovers that data it considered anonymous are still, or have once again become, personal data? How should a distinction be drawn between an error in the initial assessment and re-identification resulting from subsequent technological advances? What proactive accountability criteria, such as documentation and periodic reviews, should be applied to determine the liabilities and penalties that may arise in these situations, and which of these should apply in each case?

3. Coordination in projects involving multiple controllers

The Guidelines acknowledge that the personal or anonymous nature of data may vary depending on the perspective of each entity. In collaborative projects, this flexibility may lead to different conclusions where several independent controllers or joint controllers adopt different approaches.

Can different controllers legitimately apply different approaches and reach different conclusions regarding the same dataset? If so, how should the situation be coordinated when data are shared between entities that classify them differently?

Having common criteria would facilitate cooperation between entities, the documentation of decisions and the determination of the applicable obligations in connection with data transfers and subsequent reuse.

4. Complementarity between the Guidelines and the European Health Data Space (EHDS)

Regulation (EU) 2025/327 on the European Health Data Space (EHDS) distinguishes, in the context of secondary use, between access to anonymised health data and access to pseudonymised health data, the latter being subject to specific conditions and sufficient justification. In turn, the *Guidelines 02/2026 on Anonymisation* adopt a contextual approach whereby the classification of data as personal or anonymous depends, among other factors, on the means of identification reasonably likely to be used by the relevant entities.

The application of this approach raises a significant practical question concerning the secondary use of health data. In certain cases, a pseudonymised dataset could be considered anonymous from the perspective of the data user, if that user has no reasonably likely means of re-identifying the data subjects and no access to additional information that would make such identification possible. This raises questions as to how such classification should be reconciled with the categories and access conditions laid down by the EHDS, and how the distinction between anonymised and pseudonymised data should be preserved.

How should the contextual approach set out in the Guidelines be coordinated with the categories and conditions governing access to data for secondary use established by the EHDS? In this regard, where the data subject whose data have been pseudonymised cannot reasonably be re-identified by the data user, but can be identified by other entities, how should the nature of the data be determined for the purposes of the Guidelines and the access procedures laid down by the EHDS?

5. Coordination between the Guidelines 1/2025 on Pseudonymisation, the Guidelines 1/2026 on Scientific Research and the Guidelines 2/2026 on Anonymisation

In 2025, the *Guidelines 01/2025 on Pseudonymisation* were published. However, they do not expressly address how pseudonymisation should be coordinated with the contextual approach set out in the *Guidelines 02/2026 on Anonymisation*. Does the EDPB intend to review or update the guidelines on pseudonymisation in order to clarify when pseudonymised data should be considered personal data from the perspective of each entity?

We also ask the EDPB to clarify the relationship between Section 8.3 of the *Guidelines 1/2026 on Processing of Personal Data for Scientific Research Purposes* and the contextual approach adopted in the *Guidelines 02/2026 on Anonymisation*.

Section 8.3 of the Guidelines 1/2026 establishes that anonymisation should be prioritised where scientific objectives can be achieved using anonymous data, with pseudonymisation being used where anonymisation is not possible or proves insufficient. However, the Guidelines on Anonymisation establish that identifiability must be assessed from the perspective of each entity, taking into account the means that it may reasonably use. Consequently, data that are initially pseudonymised may not be identifying from the perspective of a particular entity.

In Example 4 of the Guidelines on Anonymisation, a hospital transmits extracts from patients' medical records to an independent research institute. Since the data are not returned to the hospital and the institute independently determines the purposes and means of the processing, the Guidelines state that identifiability must be assessed from the perspective of the institute itself.

This example raises the question of whether, if the data do not allow patients to be identified from the perspective of the receiving institute, anonymisation must nevertheless be required before the transfer, in accordance with Section 8.3 of the Guidelines 1/2026, or whether the contextual assessment of identifiability should prevail, thereby allowing pseudonymised (rather than anonymised) data to be disclosed where it is determined that the recipient cannot use them to re-identify the individuals concerned.

We therefore ask the EDPB to clarify how these approaches should be reconciled, particularly in cases where pseudonymisation makes it possible to carry out research without the receiving entity being reasonably able to identify the participants.