PUBLIC CONSULTATION SUBMISSION

Comments on EDPB Guidelines 02/2026 on Anonymisation

Submitted by DLA Piper France LLP (Data Protection & Cybersecurity) on behalf of its clients

Consultation	EDPB Guidelines 02/2026 on Anonymisation
Submitting organisation	DLA Piper France LLP - Data Protection & Cybersecurity
Date	29 October 2026

This submission consolidates practical observations raised by clients and is filed without identifying individual clients.

We welcome the opportunity to comment on the Guidelines. The three criteria of No Record Isolation, No Linkage and No Inference provide a useful framework for assessing anonymisation. Our comments seek practical clarification of their application, particularly where anonymisation takes place before disclosure to an independent recipient and where data is released repeatedly over time. The objective is to support robust, documented assessments without requiring recipients to access the personal data that anonymisation is intended to protect.

1. Source-side anonymisation and recipient assurance

Relevant provisions: sections 2.2 and 2.5.2, particularly paragraphs 11–15 and 37–41.

The Guidelines would benefit from a worked example addressing an independent recipient that has no lawful basis to receive the original personal data, including, where applicable, no relevant Article 9 condition. In that situation, anonymisation must be completed within the source environment before disclosure, rather than requiring the recipient to receive personal data in order to anonymise or validate it. Example 4, concerning the transmission of data by a hospital to an independent research institute, could usefully be developed to illustrate this situation.

We invite the EDPB to explain what evidence can provide sufficient assurance to the recipient without access to the original identifiable data. Examples could include a documented methodology, source-side test results, a description of the applicable perspectives and assumptions, and an independent assessment where appropriate. The guidance should distinguish the source controller's obligations in performing anonymisation from the independent recipient's assessment of the resulting data. We would welcome confirmation that a recipient may reasonably rely on such documented evidence, complemented by appropriate contractual commitments from the source consistent with paragraph 34, when assessing anonymity from its own perspective, as well as a practical example (e.g. Where a vendor is mandated to monitor a device for reliability and is extracting data for conducting this mission, how can said vendor ensure that the anonymisation mechanism is sufficient by not accessing the original data).

2. Scope of external information and the No Linkage assessment

Relevant provisions: sections 3.3, 3.4.2 and 3.5.2, particularly paragraphs 51, 60–65 and 88–94.

A recipient can assess the data it holds and investigate identifiable external sources, but cannot establish exhaustively what information exists in every other organisation. Further guidance would help define the reasonable scope of enquiries under the contextual approach, including when non-public information held by the source or third parties should be considered and how uncertainty should be documented.

We suggest a worked example showing how to identify relevant external datasets, assess realistic access and linkage possibilities, and record justified exclusions. We would welcome confirmation that the assessment may reasonably focus on information that relevant entities could access with means reasonably likely to be used, and need not account for purely hypothetical access to unknown datasets.

3. Hashed values and persistent identifiers

Relevant provisions: sections 2.4.1, 3.3 and 3.4.2, particularly paragraphs 23–25, 50 and 62.

Additional examples would help distinguish resistance to reversal from the ability to recognise or link the same individual over time. We invite the EDPB to address salted hashes, tokenisation and identifiers that persist across releases, including the effect of using a fresh salt for each anonymisation operation and subsequently destroying it.

The examples should explain which risks these measures address and which require separate assessment, including persistence within a release, linkage through other attributes and access to source information. We would welcome confirmation of the circumstances in which irreversible destruction of the salt or mapping, combined with the absence of persistent identifiers across releases, adequately addresses the associated linkage risk.

4. Longitudinal data and the unit of assessment

Relevant provisions: sections 3.4.1, 3.4.2 and 3.5.3, particularly paragraphs 55–57, 60 and 95–103.

Longitudinal analysis may require recognising that several observations concern the same individual without knowing that individual's civil identity. The Guidelines should explain how the definition of a record applies to all such observations, including when observations arrive through successive releases.

Paragraph 60 refers to linkage with a record "from a different dataset", whereas paragraph 65 refers to information recorded "in other contexts". Clarification is requested as to whether successive releases from the same source constitute a single dataset or different datasets for the purposes of the No Linkage criterion.

We request an example distinguishing linkage between observations within the assessed data, linkage to a separate dataset, and identification or singling out in the relevant context. The example should show when a failed technical criterion requires further analysis rather than an automatic conclusion that the data is personal. It should also explain how accumulating attributes can change the assessment even where each release was assessed separately.

5. Cumulative releases, rare events and reassessment

Relevant provisions: paragraphs 35, 67–82, 85–88 and 102.

Further operational guidance is needed on assessing successive releases together. We suggest examples addressing overlapping populations, repeated releases, differences between aggregate releases and the progressive accumulation of attributes. These should explain when a new release calls for reassessment of earlier data and how the source and an independent recipient can exchange the necessary assurance information without disclosing identifiable data.

An example involving a rare event within a larger group would also be helpful. The guidance should distinguish a statistical observation about a group from a specific and meaningful inference concerning an identified or identifiable individual, taking account of external information and membership inference. We would welcome confirmation that a documented minimum group-size threshold, applied consistently, is a relevant factor in demonstrating that no specific and meaningful inference can be drawn.

Finally, we invite the EDPB to describe proportionate reassessment triggers, such as a new release, a material change in available external information, or a change in access conditions. We would welcome confirmation that a periodic cumulative review, documented at reasonable intervals, is an acceptable

approach to demonstrating that the assessment covers the data cumulatively available, rather than only each release in isolation.

These clarifications would make the framework easier to apply consistently while preserving its contextual legal standard and the protection of individuals.

DLA Piper France LLP
Data Protection & Cybersecurity