30.10.2026

FiCom ry

FiCom comments on EDPB Guidelines 02/2026 on Anonymisation

FiCom represents companies in Finland's telecommunications and digital communications sector. We welcome the EDPB's effort to clarify when data can be considered anonymous. Anonymisation protects individuals while enabling the use of information for network planning, service quality and research. The legal threshold should remain practical and predictable: it should be based on means reasonably likely to be used for identification, not on every theoretical possibility.

FiCom supports the recognition that anonymity depends on the relevant entity's perspective.

FiCom calls on the EDPB to clarify the contextual legal test, set realistic limits for identification chains, recognise the practical effect of safeguards, ensure proportionate reassessment, and confirm that the simplified approach is optional. The Guidelines should also include examples on communications network and mobility data.

The contextual assessment must remain the legal benchmark

The Guidelines correctly recognise that identifiability must be assessed in context. The same information may be personal data for one entity and anonymous for an independent recipient. This matters when an operator provides aggregated data to a research or planning organisation that has no reasonably likely means to identify subscribers.

The Guidelines also confirm that the simplified approach is voluntary and is not a separate legal standard. It may assist an initial assessment but can classify data as personal even when they are anonymous under the GDPR. Regulators should therefore not treat it as mandatory. Failure of a No Record Isolation or No Linkage test requires further assessment and is not conclusive evidence of identifiability. This distinction should also be made clear in the flowchart in Annex 1 and in Guidelines at a Glance, so that the simplified approach is not treated as a mandatory legal standard.

Potential recipients and identification chains need clearer limits

In line with the Court of Justice's case-law on identifiability, the EDPB should clarify that both the likelihood of onward transfer and the recipient's means of identification must be assessed in light of objective circumstances. This would avoid extending the assessment to speculative identification chains involving hypothetical recipients or merely conceivable combinations of information.

The assessment should also distinguish an independent recipient from a processor acting for the original controller. Data may be anonymous for an independent recipient while the originating controller remains responsible for processing and disclosure of the underlying personal data.

Safeguards and reassessment should be proportionate

Contractual restrictions, technical controls and organisational measures do not automatically establish anonymity. Their combined practical effect is nevertheless relevant when assessing which actors can obtain data or information needed for identification through means reasonably likely to be used. The final text should illustrate how such safeguards affect practical access. A hypothetical security incident should be decisive only where objective circumstances support a credible threat scenario.

Changes in technology or access to auxiliary information may affect anonymity. Reassessment should be proportionate to the relevant risks and carried out when warranted, including following material changes in technology, available auxiliary information or the release of data. The Guidelines should not be understood as requiring indefinite monitoring of every anonymous output regardless of its sensitivity, use or exposure.

Add examples for communications network and mobility data

The Guidelines would benefit from a telecommunications example. Operators produce statistics on network utilisation, traffic volumes and service quality by area and time period for planning, optimisation and research. Properly aggregated results may describe network performance or groups of users without identifying individuals. The example should show how output granularity, population size, auxiliary information, access arrangements and the intended recipient's realistic capabilities affect the conclusion on whether the output is anonymous.

Location-related information needs particular attention because small populations, precise areas, repeated observations and detailed movement patterns may create identification risks even after direct identifiers are removed. The EDPB should show how aggregation, suppression of small groups, reduced spatial or temporal resolution and controlled disclosure can address these risks without imposing one threshold on all datasets. It should also distinguish an anonymous output's status under the GDPR from sector-specific confidentiality and traffic- or location-data requirements governing the earlier processing.

FiCom therefore asks the EDPB to preserve the contextual, evidence-based approach throughout the final Guidelines. This would support effective data protection while allowing the responsible use of genuinely anonymous data.