31 July 2026

Van Bael & Bellis

Anonymisation: Key Takeaways from the EDPB's Draft Guidelines

On 7 July 2026, the European Data Protection Board published its draft Guidelines 02/2026 on Anonymisation (the ***Guidelines***). The Guidelines set out what qualifies as anonymous data and offer a practical framework for assessing whether anonymisation has been carried out successfully. The Guidelines update the Article 29 Working Party Opinion 05/2014 on anonymisation techniques. They reflect significant developments in the case law of the Court of Justice of the European Union (CJEU), in particular the EDPS v SRB decision (C-413/23P – see our Client Alert, CJEU Clarifies Concepts of Personal and Pseudonymised Data, 11 September 2025) as well as advances in artificial intelligence and the emergence of EU-wide data spaces.

Legal Analysis - the Core Questions

The assessment of whether information is anonymous involves two questions: (i) does the information "relate" to a natural person and, if so, (ii) is that person "identified or identifiable". If the answer to either of these questions is "no", then the data should be considered anonymous. Importantly, the outcome of this test is entity-specific: data may be anonymous for one entity but not for another.

Whether information "relates" to a person depends on three elements.

First, the content, which concerns information that is about the person per se, describing one or more of their characteristics or actions (e.g., an employee record, a patient's medical record, etc.).

Second, the purpose, which covers information that, while not necessarily about that person per se, is used (or likely to be used) to evaluate, treat or influence that person's status or behaviour. This may include information about an object (e.g. a car), an organisational entity (e.g. an association), or a relative (e.g. a friend or a family member).

Third, the effect, which relates to information whose processing is liable to have an impact on the person's rights and interests, creating a concrete possibility that the person can be treated differently from others (e.g., location data of taxis that is collected for the purpose of optimising itineraries, but which also allows for the monitoring of the taxi drivers' performance).

The second question asks whether the person can be singled out within a given context, whether through direct identifiers or a combination of attributes. Identification may be direct (an entity can identify a person using its own means) or indirect, where the entity could identify the person through means reasonably likely to be used, such as (i) by obtaining additional information, (ii) by applying methods controlled by other parties such as decryption; and/or (iii) by making the data available to other entities that have themselves means reasonably likely to be used to identify that person.

The Guidelines clarify that information does not need to carry a zero risk of identification to qualify as anonymous. Instead, the likelihood of successful re-identification must be insignificant. This may be the case where identification is impossible, would require disproportionate time, cost or effort, or is prevented by a legal prohibition. Importantly, a contractual prohibition, even if binding upon the parties, does not carry the same weight.

Technical Analysis – the Three Criteria Assessment

Where the answer to the identifiability question is not straightforward, the Guidelines recommend a technical assessment informed by current re-identification techniques. This assessment may follow one of two approaches.

First, the contextual approach, based on the legal analysis and taking into account the means of each relevant entity and the likelihood that those means would in practice be used to re-identify individuals. Second, the simplified approach, which disregards differences between entities and applies a uniform standard. In that case, it can lead the anonymising controller to treat the data as though it is not anonymous even if it would actually be so for the relevant entities.

Under both approaches, the technical analysis is structured around three criteria:

i. No Record Isolation, meaning the data does not contain any combination of attribute values that uniquely points to a single person. The more attributes a record contains, the higher the risk of uniqueness. Example: a company shares an anonymised HR dataset from which names and employee numbers have been removed, with each record showing department, seniority level, contract type, and salary band. If only one individual in the dataset is a part-time Director in the Legal department within a given salary band, that combination of attributes is unique and points to that person alone. In that case, this criterion is not met.
ii. No Linkage, meaning it must not be possible to connect a record in the dataset to other records about the same person held in separate datasets. Example: a retailer removes customer names and email addresses from a purchase dataset but retains postcode, product category, and purchase date. A loyalty programme database held by a partner contains the same combination of attributes linked to named individuals. Because records in the two datasets can be matched on those shared attributes, this criterion is also not met.
iii. No Inference, meaning the data must not allow any specific and meaningful inference to be drawn from the given data whether on the basis of the dataset alone or in combination with external sources. Example: a company reports that its six engineers earn €550,000 in total and that the five engineers on the Product Engineering team (which does not include any other employee) account for €480,000. Although both figures are aggregated, they allow the salary of the remaining engineer to be inferred as €70,000.

If all three criteria are satisfied, the data may be regarded as anonymous. Failing one or more criteria does not, however, automatically render the data personal but triggers a more detailed assessment of whether the failure in question creates a genuine risk of identification.

Practical Implications

The Guidelines provide welcome clarity for organisations seeking to use anonymised data outside the full scope of the GDPR. However, anonymisation is itself processing and must therefore have a valid legal basis under Article 6 GDPR or, for special category data, under Article 9(2). Controllers must also inform data subjects that their data will be used to produce anonymous information and must avoid labels such as "anonymous", "de-identified" or "de-personalised" where individuals remain identifiable.

Robust documentation of the anonymisation process is essential, both to demonstrate GDPR compliance and to assess the effectiveness and resilience of the measures applied. In addition, anonymisation should not be treated as a one-off exercise. As artificial intelligence and re-identification techniques continue to develop, the risk of re-identification may increase over time. Periodic reassessment of anonymised datasets is therefore recommended.

The Guidelines are available here (in English). VBB stands ready to assist organisations wishing to submit their views before 30 October 2026.

Key contacts

Tanguy Van Overstraeten
Partner
tvanoverstraeten@vbb.com

Malik Aouadi
Associate
maouadi@vbb.com

Habiba Daher Ahmed
Associate
hdaherahmed@vbb.com

Brussels
Glaverbel Building
Chaussée de La Hulpe 166
B-1170 Brussels
Belgium
+32 (0)2 647 73 50

Geneva
2 Chemin des Mines
CH-1202
Geneva
Switzerland
+41 (0)22 320 90 20

London
Holborn Gate
330 High Holborn
London, WC1V 7QH
United Kingdom
+44 (0)20 7406 1471

www.vbb.com