DIGITALEUROPE

30 October 2026

# Recognising successful data anonymisation

## Executive summary

DIGITALEUROPE welcomes the European Data Protection Board (EDPB)'s initiative to draft guidelines on anonymisation, aiming to provide a practical framework to succeed in anonymising data.[1] As the guidelines are being developed in the midst of the Digital Omnibus negotiations, they will have a direct impact in the ongoing debate.[2] The Guidelines should expressly specify that they do not pre-empt the ongoing Digital Omnibus legislative negotiations concerning the definition of personal data and the application of the entity-relative standard to processors. The EDPB should coordinate with other EU institutions, such as the AI Office, and commit to a formal post-adoption review once the Digital Omnibus is enacted.

In February 2026, DIGITALEUROPE issued recommendations with regards to the proposed changes under Digital Omnibus.[3] Targeted changes, based on the GDPR's application for over 8 years, can help clarify the different legal bases for innovation and security, define pseudonymisation and codify existing guidance and case law. Regarding anonymisation in particular, the EDPB has a key role to play to ensure the harmonised application of the GDPR. We recommend amendments to the guidelines, to ensure that they are clear enough and can be easily picked-up by industry but also consistently applied by all Data Protection Authorities (DPAs), in line with the Helsinki declaration. We recommend the guidelines:

- Remove any additional layers of complexity brought by the multiple tests proposed, notably by recognising both tests' full efficiency.
- Recognise the legal weight of contractual obligations and obligations stemming from other legislations than the GDPR, applicable to the same data. In order to achieve this, the EDPB could conduct wholistic assessment of the legislative framework that applies to the digital sector alongside the GDPR.

[1] Guidelines 02/2026 on Anonymisation (V1.0)

[2] COM(2025) 837 final.

[3] See DIGITALEUROPE, *Digital omnibus: a first step and what must come next, now*, available at https://cdn.digitaleurope.org/uploads/2026/02/Digital-omnibus-a-first-step-and-what-must-come-next-now.pdf .

**DIGITALEUROPE**
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

- Are amended to ensure coherence with the risk-based approach throughout the processing of data made anonymous, especially with regards to the risk of unlawful access, the legal basis and assessing the perspective of the controller.

- Further reinforce the applicability of different assessments when considering the technical analysis of anonymisation.

# Table of contents

**Executive summary** ..... **1**
**Table of contents** ..... **3**
**Avoiding new layers of complexity** ..... **4**
**Legal and contractual obligations** ..... Error! Bookmark not defined.
**Coherence throughout processing** ..... **6**
**Technical criteria** ..... **7**

# Avoiding new layers of complexity

## Practicality of multiple tests

While we welcome the flowchart proposed on the last page of the draft guidelines, the multitude of tests and alternative standards remain complex. While a unified approach would have ensured more clarity, we recommend that the efficiency of both approaches be equally recognised. For instance, the analysis proposed by the guidelines of 'content, purpose, effect' to assess whether data 'relates' to an individual does not fit the flowchart, and could be removed, unless reflected in the flowchart.[4]

In a further effort to simplify the Guidelines, the text should clarify that identifiability may be assessed by reference to a specific department, function or entity that carries out the processing. This is hinted at under paragraph 5 and under Section 2.2, but the assessment should consider whether identifying information elsewhere within an organisation is realistically likely to be used by the relevant processing operation, taking into account technical segregation, access controls, governance arrangements, personnel separation and/or the purposes for which the information is processed..[5]

## Likelihood of re-identification, in practice

The guidelines add a new obligation on entities that process anonymised data: to assess the likelihood that re-identification techniques may further be developed. This prediction would be made on a constant basis and at least with periodical reviews. The GDPR mandates regular reviews in certain defined cases, such as where an impact assessment is required, but not to predict the development of new re-identification techniques.

Instead of adding a new burden of constant re-assessments and predictions, the guidelines should only require re-assessments that are proportionate to actual material changes, such as new auxiliary datasets, significant change in access, or security incidents. Additionally, other existing tools under the GDPR, such as processor obligations under Art. 28 GDPR, Codes of conduct under Art. 40 GDPR and certifications under Art. 42 GDPR should be included in the assessment of the risk of onward access or re-identification.

Last, the draft guidelines currently place the risk of accidental or negligent access at the same level as unlawful attempts to access data with ill-intent. The operational and contractual measures actually in place to prevent unlawful access should instead be relied upon to measure risk of accidental or negligent access. Indeed, in practice, parties can effectively set preventive measures, but they cannot predict every risk of ill-intent-from rogue employees to investigative journalism.[6] Placing ill-intent at the same level as accidental or negligent access would put into question the value of contractual obligations.

## Treating anonymised data as personal data

By stating that the simplified approach developed by the guidelines would lead to wrongly treat anonymised data as personal data, the draft guidelines acknowledge limitations to the test. Companies should not be encouraged to support false positives, while also being encouraged to boost the European

[4] Para 16

[5] Recital 26 focuses on means likely to be used

[6] Para 30, 31, 33

data market and innovate based on non-personal data.[7]Anonymous data often has high economic value and should not be incorrectly classified and lost..[8]

### Examples

The numerous examples proposed by the guidelines reflect the EDPB's objective to bring more practical guidance. It would be of further help to provide the use case tied to AI model development and training, on the use of synthetic data and on privacy-enhancing technologies. Additionally, some of the examples do not provide solutions to the party involved. For instance, example 3 could provide more information as to the safeguards in place which could ensure anonymisation and specifically which data was provided to the agency, which data and systems it has access to and which technical and contractual safeguards were in place. Existing techniques to anonymise and pseudonymise data could also be mapped in the examples, as Privacy Enhancing Technologies are increasingly developed and are being considered within the Omnibus discussions.

## Legal and contractual obligations

Under paragraph 29, when having to assess the means another party might have to identify an individual, a party may have to consider 'reasonably foreseeable technological developments'. This is reinfroced by the statement that the likelihood of re-identification typically increases over time, due to advances in technology.[9] This interpretation is far-stretching, and the paragraph fails to reference concrete and predictable safeguards, such as contracts or legislative provsisions, that prevent the misuse of data to identify a person. Factors that decrease the likelihood of identification should be given due consideration, to avoid an overly cautious approach, treating anonymised data as personal data.

The mere possibility that contractual terms could be amended or breached in the future should not outweigh the objective safeguards in place at the time of the assessment. Non-personal data sharing most often takes place on the basis of contracts, in B2B but also in B2C settings. This is also consistent with EU policy more broadly, included long promoted contractual data sharing agreements, notably by developing the FAIR principles, Standard Contractual Clauses and Model Contractual Clauses. Similarly, past EDPB guidelines have referred to contractual requirements, and recognised their force for instance to limit onward sharing of data received by third party undertakings.[10]The GDPR itselft refers to contractual obligations under Art. 6(1)(b). Contracts should therefore be fully recognised as a way to restrict re-identification, and a reliable basis. We recommend deleting paragraph 34 that undermines contractual freedom and legislation that requires contractual agreements. If not, the text must be substantially amended to state that enforced and monitored contractual obligations carry decisive weight, alongside technical measures.

[7] See European strategy for data (https://digital-strategy.ec.europa.eu/en/policies/strategy-data)

[8] Para 45

[9] Para 35

[10] See Para 189 of the recent joint guidelines on the interplay of the GDPR with the DMA.

The guidelines should avoid cautioning against the 'lack of motivation' test when the rule of law would prevent misuse of data. We recommend that the guidelines clarify they are referring to one particular case, Breyer C-582/14, in the body of the text rather than as a more elusive reference.[11]

Additionally, we recommend deleting the reference to evidence intended to rebut the presumption of legality. The relevant question under Recital 26 is whether identification is reasonably likely to be used in the circumstances, taking account of the legal framework that applies to the parties. Indeed, considering whether a party may or may not follow the law goes beyond the obligations under the GDPR and should be removed. [12]

## Coherence throughout processing

Although the draft guidelines show a level of openness to different levels of risk, we would welcome a more coherent approach, especially regarding the legal basis parties can rely on to anonymise data and use it. The guidelines are an opportunity to help parties avoid over-anonymising data, and properly use anonymisation including for mixed datasets.

### Legal basis

The last sentence of paragraph 38 should be clarified: while we welcome the confirmation that one same legal basis can be presumed to apply for anonymisation as for the processing of special categories of data if part of the same processing activity, the reference to 'the same purposes' at the end of the sentence confuses the message. Indeed, it would imply that the presumption only applies for the same processing activity as the original purpose.

### Defining the perspective

The draft guidelines require that an entity processing on behalf of another should assess whether the personal data is anonymised from the perspective of the controlling entity.[13] This goes beyond CJEU case law and in particular the EDPS v. SRB case, that notes that depending on the circumstances of the case, persons other than the controller can be prevented from identifying the data subject. The controller can set safeguards for instance through technical and organisation measures, or contractual obligations.

A recipient-focused assessment would not create an outsourcing loophole, as the controlling entity would continue to treat data that is identifiable from its perspective as personal data. The processing entity could regard the information as anonymous only where the data, instructions, technical controls and auxiliary information actually available to it leave no means reasonably likely to be used for identification. If the controller later provides identifying information or a key, the position must be reassessed and the GDPR would apply to the relevant processing.

[11] Para 31 identifies only one example where 'an entity is forced by outside circumstances' to identify an individual, and applies it as a general risk.

[12] Para 33

[13] Para 15

We do, however, support the recognition that information simply relating to a person will not automatically be classified as personal, as in most cases data is anonymised to learn a limited amount of information about a person without identifying them.[14] For the same reason, we welcome the affirmation that the risk of successfully distinguishing an individual from others does not need to be zero.[15]

### Mixed datasets

Within paragraph 36, we recommend changing the grammatical phrasing from 'the entire dataset' to 'the dataset as a whole', to avoid suggesting that all the data within the dataset is no longer anonymous including when parts of it can be separated. Indeed, the draft Guidelines then state that 'in any situation where the separate parts of the dataset are not treated separately'.

## Technical criteria

When describing the test for no record isolation, the draft guidelines conclude that even if data passes the test, the attributes could still be linked to other datasets and hence violate the test for no linkage. We recommend clarifying that here, if the appropriate controls are in place the second test for no linkage can also still be passed. [16] this would be particularly helpful as example 11 does not provide a solution for the controller to fulfil the no-linkage test.

In considering accessibility of data that is publicly available, the draft guidelines helpfully distinguish the means that authorised and unauthorised users may have to access the data.[17]However, they fail to recognise other standardised access restrictions or controls, and instead, controllers are encouraged to adopt technical, organisational and contractual measures, without the assurance that such measures would actually support the conclusion that data are anonymous. [18] We recommend that the guidelines clarify that robust encryption, key separation and control access constitute effective barriers, that deprive the recipient of the means reasonably likely to identify data subjects.

[14] Para 18

[15] Para 22

[16] Para. 63

[17] Para 89

[18] Para 90

FOR MORE INFORMATION, PLEASE CONTACT:

Beatrice Ericson

**Senior Policy Manager**

beatrice.ericson@digitaleurope.org / +32 492 25 84 32

THE VIEWS EXPRESSED IN THIS STUDY ARE THOSE OF DIGITALEUROPE AND DO NOT NECESSARILY REFLECT THE POSITIONS OF ITS INDIVIDUAL MEMBER ORGANISATIONS OR CONTRIBUTORS.

## About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European digitalising businesses across multiple sectors and citizens to prosper from digital technologies. We wish for Europe to grow, attract and sustain the world's best digital talents, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters, and contribute to their development and implementation. Our membership represents over 56,000 businesses who operate and invest in Europe. It includes corporations and scaleups who are global leaders in their field of activity, as well as national trade associations from across more than 30 European countries.

**DIGITALEUROPE**
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

@DIGITALEUROPE DIGITALEUROPE digitaleurope_org