CIPL Response to the European Data Protection Board's Public Consultation on Guidelines 02/2026 on Anonymisation

Centre for Information Policy Leadership (CIPL)

30 October 2026

CIPL Response to the European Data Protection Board's Public Consultation on Guidelines 02/2026 on Anonymisation

The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines 02/2026 on Anonymisation (the "draft Guidelines"), adopted for public consultation on 7 July 2026.[1] CIPL commends the EDPB's efforts to bring greater clarity to an area that has been uncertain for organisations for many years.

Anonymisation plays a crucial role in European data policy, enabling the use and re-use of data for research, public health, statistical analysis, fraud prevention, developing and improving services, and the development and evaluation of AI systems. Where anonymisation proves unattainable in practice, organisations are often left to choose between processing under the full weight of the GDPR or forgoing those uses altogether. The standard the EDPB adopts therefore determines not only the scope of the Regulation, but equally the extent to which organisations are encouraged to invest at the outset in the technical measures that reduce identifiability.

CIPL has for a number of years advocated an update to the 2014 guidance on anonymisation. That update has now become imperative to reflect not only a decade of technological, policy and legal development, but also the Court of Justice's judgment in *EDPS v SRB*, which confirmed an entity-relative, recipient-focused approach to identifiability.[2]

The draft Guidelines provide a number of helpful clarifications. CIPL particularly welcomes the entity-relative, contextual approach, which reflects the Court's most recent case law and recognises that the same dataset may be anonymous in the hands of one entity and personal in the hands of another. CIPL also welcomes the confirmation that the likelihood of identification need not be reduced to zero, but to a level that is insignificant in reality.[3] The three criteria of *No Record Isolation*, *No Linkage* and *No Inference* introduce a level of clarity, and the acknowledgement that the violation of a criterion does not, of itself, render data personal is a welcome nuance.

Yet on the central question of when identification is reasonably likely, the draft develops the factors that increase the likelihood of identification at length, while the considerations that reduce it are dispersed across the text and are not drawn together into a framework allowing for clear weighing of the two. The same imbalance runs through the treatment of unauthorised actors, future developments and safeguards. Carried into the final text, that imbalance would push organisations towards treating data as personal by default, without a corresponding benefit to individuals.

The timing of the draft Guidelines also poses a challenge. The meaning of "anonymised" is currently being settled on several fronts at once: administratively, in the Commission's specification proceedings under Article 6(11) DMA[4]; judicially, as courts and supervisory authorities apply the Court's recent case law; legislatively, through the Digital Omnibus; and in these draft Guidelines. CIPL

[1] EDPB, Guidelines 02/2026 on Anonymisation, version 1.0, adopted 7 July 2026.

[2] Judgment of 4 September 2025, *European Data Protection Supervisor v Single Resolution Board*, C-413/23 P, building on Judgment of 19 October 2016, *Breyer v Bundesrepublik Deutschland*, C-582/14.

[3] Draft Guidelines, para. 22, citing C-413/23 P *EDPS v SRB*, para. 82.

[4] Case DMA.100209 – SP – Alphabet – Article 6(11), available at https://ec.europa.eu/competition/digital_markets_act/cases/202637/DMA_100209_2799.pdf.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

has consistently argued that the concept should carry a single, GDPR-consistent meaning across the EU's digital acquis.[5]

The comments below identify where further clarification and practical guidance would help. They focus on the practical end of anonymisation: the points at which an organisation acting in good faith, or a supervisory authority reviewing an assessment, may find the draft challenging to apply consistently. They also point to internal inconsistencies and to areas where greater legal certainty is needed. This is in keeping with the EDPB's commitment, in its Helsinki Statement, to practical guidance that makes compliance easier.[6]

1. One concept to be determined across parallel processes

CIPL has long advocated for an update to Opinion 05/2014 and welcomes the fact that the EDPB has taken this work forward. Organisations have been applying a framework that predates both the current case law and the present generation of re-identification techniques. The draft is nonetheless published at a moment when the same question is being settled elsewhere, and not always consistently:

- **Under the DMA.** The European Commission has recently adopted its specification decision in Case DMA.100209. That decision gives the anonymisation requirement under Article 6(11) DMA a practical meaning. It sets out a defined sequence of technical measures, including a grouping threshold, complemented by contractual restrictions that require recipients to process the shared dataset in a segregated environment which prevents linkage with auxiliary data. In the Commission's formulation, the technical measures reduce the risk of re-identification to a residual level, and the contractual measures then carry the decisive step from residual to insignificant.[7] CIPL has questioned that balance, since there is a difference in kind between measures that change what the data is and measures that govern only what a recipient may do. Moreover, the DMA does not establish a self-standing notion of anonymisation. The DMA applies without prejudice to the GDPR, which provides the governing standard, and the anonymisation required under Article 6(11) DMA must therefore be anonymisation within the meaning of the GDPR.[8]
- **Judicially.** The Court settled the entity-relative, recipient-focused approach to identifiability only in September 2025, and its application by national courts and supervisory authorities is still being worked out.
- **Legislatively.** The Digital Omnibus proposes amendments that bear directly on the analysis in sections 2.2 to 2.4 of the draft Guidelines. These include an amended Article 4(1) GDPR codifying an entity-relative approach to identifiability, and a new Article 41a empowering the Commission to specify by implementing act when data resulting from pseudonymisation ceases to be personal

[5]CIPL, A Single Standard for Anonymisation: Article 6(11) DMA and the GDPR (July 2026); see also CIPL, Data Sharing Obligations Under the DMA: Challenges and Opportunities (May 2024), and CIPL, Response to the European Commission and EDPB Public Consultation on the Draft Joint Guidelines on the Interplay between the DMA and the GDPR (December 2025).

[6] EDPB, The Helsinki Statement on enhanced clarity, support and engagement, 2 July 2025.

[7]Case DMA.100209 – SP – Alphabet – Article 6(11), available at https://ec.europa.eu/competition/digital_markets_act/cases/202637/DMA_100209_2799.pdf.

[8]Recital 12 DMA confirms that the DMA applies without prejudice to the GDPR. See also European Commission and EDPB, Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation (version for public consultation), and CIPL, A Single Standard for Anonymisation (July 2026).

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

data for certain entities.[9] Both provisions remain under negotiation, on a timeline that extends beyond the adoption of these Guidelines.

Two risks follow from reading these Guidelines in isolation from those developments.

- The first is divergence: a single concept acquiring one meaning as applied to a mandated data-sharing obligation under the DMA and another under the GDPR. It is difficult to see how the same dataset could sensibly be treated as anonymous for the purposes of one instrument and as personal data for the purposes of another.
- The second is the prospect of guidance requiring revision within a year of its publication, which would itself become a source of the very uncertainty the Guidelines are intended to dispel, particularly for organisations that may by then have taken architectural and investment decisions in reliance upon them.

The EDPB and the Commission, as well as other relevant institutional stakeholders, should strengthen cooperation and ensure that the standard they establish is a single standard of anonymisation across EU law, including where "anonymised" appears in the DMA, the Data Act and other instruments of the digital acquis. That is a question for the EDPB, the Commission and national authorities together, with technical expertise on both sides, rather than one to be settled in a competition-enforcement file and a separate set of EDPB guidelines. CIPL would encourage the EDPB, at a minimum, to include a commitment to review the Guidelines once the Digital Omnibus has concluded and the DMA standard has settled.

2. The likelihood standard should be applied in both directions

The draft Guidelines helpfully reflect the Court's assessment in *EDPS v SRB* and *Breyer*, under which means are not reasonably likely to be used where the risk of identification appears in reality to be insignificant, whether this is because

- identification is prohibited by law;
- it would be impossible in practice; or
- it would involve disproportionate effort in terms of time, cost and labour.[10]

Paragraph 29 helpfully identifies a list of objective factors relevant to assessing the likelihood of identification, but the draft develops the factors that increase the likelihood more fully than those that reduce it. Paragraphs 30, 31 and 33 elaborate on the breadth of potential adversaries, the limits of relying on lack of motivation, and the relevance of legal prohibitions. Factors pointing in the opposite direction, including effective and permanent restrictions on access, the costs and time of identification, the risks that re-identification would create for the re-identifying entity, and access controls, are recognised but dispersed across paragraphs 29(b), 29(d), 31, 89 and 90. The draft should pull these considerations together and also offer guidance on how factors of increasing or decreasing likelihood are to be weighed against one another.

That imbalance is reinforced by the breadth with which the draft defines the relevant means. Paragraph 28 describes means as covering anything from simply reading a document to making a web

[9]Digital Omnibus package, published 19 November 2025, proposing an amended Article 4(1) GDPR and a new Article 41a empowering the Commission to specify by implementing act when data resulting from pseudonymisation no longer constitutes personal data for certain entities.
[10]C-413/23 P *EDPS v SRB*, para. 82; C-582/14 *Breyer*, para. 46.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

search to running "incredibly complex analyses and inferences".[11] Read together with the draft's approach to indirect chains of means, unauthorised and malicious actors, and reasonably foreseeable technological developments, this risks blurring the distinction between the theoretical possibility of identification and identification for which means exist that are reasonably likely to be used. The Guidelines should not set a bar which goes beyond the Court's contextual standard by focusing on what is technically conceivable in the abstract.

A related question arises with respect to paragraph 21. There the draft Guidelines provide that where it is reasonably likely that an entity can transfer the data to a third party, and it "cannot be ruled out" that the receiving entity has the means to identify the individual through means reasonably likely to be used, the data should be considered personal both for that transfer and for the recipient's subsequent processing.

Paragraph 22, immediately following, confirms that the likelihood of identification need not be zero, but should be insignificant in reality. The substantive test is therefore unchanged; what differs is the burden. Ruling out identification and reducing its likelihood to an insignificant level are not the same thing: the first asks for certainty, the second for an assessment of likelihood. Paragraph 21 requires the transferring entity to show a negative about a recipient's capabilities at the moment of sharing, which is where anonymisation is most often deployed. Read strictly, an entity sharing de-identified data would find that requirement difficult to satisfy in any but the clearest cases. The final Guidelines should align paragraph 21 with paragraph 22, so that the question is whether identification by the recipient is reasonably likely, not whether it can be excluded.

Paragraphs 20 and 21 also conflate capability with likelihood, asking whether an entity "could" obtain additional information or "can" transfer data. Recital 26 GDPR asks instead which means are reasonably likely to be used, and paragraph 29 itself refers to "the likelihood of their actual use". The theoretical ability to take a step does not make it likely to be taken. Where a controller shares pseudonymised data but keeps the key, that key is subject to the safeguards in Article 4(5) GDPR, and disclosing it would be a new processing operation requiring its own legal basis. These are objective legal and technical constraints, not a question of motivation. The final Guidelines should confirm that, absent concrete evidence that the key will be disclosed, the mere possibility of disclosure does not make the data personal for the recipient, including within a corporate group, consistent with *EDPS v SRB*.[12]

The draft Guidelines provide a structured list of risk-increasing factors, but no comparable framework for demonstrating that risk has been reduced to an insignificant level. Examples 22 and 24 provide limited assistance. Compliance teams might lean towards classifying data as personal by default as a result, which ultimately negates the significance of that classification, reduces the incentive to invest in technical de-identification, and has the potential to restrict beneficial uses of appropriately protected data without a corresponding benefit to individuals.

The final Guidelines should instead set out a non-exhaustive framework for applying the likelihood standard in both directions, giving equal and proportionate consideration to the circumstances that decrease the likelihood of identification and those that increase it. Alongside the factors in paragraph 29, the Guidelines should identify the considerations that reduce realistic identifiability. These should include the availability, quality and currency of auxiliary data; the cost, time, expertise and computational resources an identification attempt would require; the access conditions and the technical, organisational and contractual safeguards in place; whether information needed for

[11]Draft Guidelines, para. 28. See also para. 20 on indirect identification and chains of means, para. 30 on unauthorised and malicious actors, and para. 29(e) on reasonably foreseeable technological developments.
[12] C-413/23 P *EDPS v SRB*, paras. 79 and 87; draft Guidelines, paras. 20, 21 and 29 and footnote 7.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

identification is held separately under binding restrictions on its disclosure; whether the data is used only for aggregate outputs; the accuracy and confidence a technique would achieve; and the practical probability that an attempt would succeed. The analysis should be directed towards concrete means that exist or are reasonably foreseeable in the specific circumstances, rather than open-ended factors that are merely technically conceivable. This is particularly important where the data is not made publicly available, since the range of entities with realistic access is then considerably narrower. The EDPB should confirm that the assessment must be holistic, that no single factor is dispositive, and that the question is in all cases whether identification is reasonably likely in the concrete circumstances, rather than conceivable in the abstract.

A similar concern arises in the way the draft Guidelines interpret "effort". Paragraph 26 recognises that identification requiring disproportionate effort in terms of time, cost and labour is not reasonably likely. Paragraph 92, however, states that time and cost would not generally be prohibitive for running existing re-identification techniques, and paragraphs 92 and 93 anticipate that developments in AI will reduce both further. Read together with paragraph 29(e) on foreseeable technological developments and paragraph 88 on safety margins, these general observations risk prejudging the assessment of effort before the facts of a particular case are considered. The final Guidelines should make clear that effort is assessed from the perspective of the relevant entity in the specific circumstances, that any account taken of foreseeable developments or safety margins should rest on concrete evidence, and that later advances in re-identification capability are a matter for reassessment.

2.1 Unauthorised and accidental access should be assessed against realistic pathways

Paragraph 30 lists the entities with potentially relevant means: receiving entities, rogue employees, friends and family, investigative journalists, law enforcement and intelligence agencies, unethical companies and cybercriminals. CIPL agrees that such actors cannot be categorically excluded. CIPL appreciates that the draft recognises, in a footnote to paragraph 30, that not all of these perspectives need to be considered systematically in each case, and the closing passage of that paragraph distinguishes between entities that can supply additional information and those that can access the given data or run the necessary technology. That qualification is important and would carry greater weight in the main text than in a footnote, accompanied by an indication of what must be shown before an actor is treated as relevant. Listing an actor is not the same as showing that data will be obtained and lead to a successful identification. Paragraph 89 goes further: where appropriate security controls are in place, only authorised users are treated as having access to the data through means reasonably likely to be used.

That principle is absent from paragraphs 30 and 31. Paragraph 31 also brings accidental and negligent identification into the analysis without further information as to when this is significant, so that on a literal reading any imaginable mistake counts. Example 22 is helpful in that context: the research institute considers who might realistically receive the data following a leak, and concludes that people familiar with the data subjects' personal lives would not qualify as relevant entities. However, that reasoning should be stated as a principle rather than left to a single example.[13]

More generally, unauthorised access and accidental disclosure should be relevant only where the facts show a realistic likelihood of both access to the given data and successful re-identification. This is an evidential question, turning on the actual means of access, the actor's capabilities, the strength and testing of security controls, incident history in comparable settings, monitoring and enforcement, incentives, and the practical likelihood that an attempt would succeed. Paragraph 31 should confirm

[13]Draft Guidelines, paras. 30 and 89, footnote 25 and Example 22.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

that an accident or negligent act is relevant only where it is reasonably foreseeable in the circumstances, rather than merely conceivable. Likewise, where the security controls described in paragraph 89 are in place, unauthorised actors should be relevant only on concrete evidence that those controls could realistically be circumvented.

2.2 Legal prohibitions should retain the weight the Court has given them

The draft Guidelines reiterate in paragraph 32 that the Court considers means prohibited by law as not satisfying the "reasonably likely to be used" standard, and accept that it may generally be assumed that people will follow the law. Paragraph 33 then appropriately sets out the threshold for rebutting that assumption, requiring sufficient evidence of a concrete risk, in particular evidence that the prohibition is not respected by the entities involved. CIPL would like to point out, however, that the factors subsequently listed are drawn more broadly than that test. A prohibition laid down in law is a prohibition. The Union is founded on the rule of law, and compliance with binding legal obligations is the premise on which the GDPR itself stands. Whether a given law is adequately supervised and enforced, and whether a third party might conclude that breaching it would be worthwhile, are questions for legislators and for the authorities responsible for enforcement. Controllers cannot answer them, and answers that rest at best on an educated guess do not meet the evidential threshold for a concrete risk that paragraph 33 itself requires.[14]

CIPL would encourage the EDPB to confirm that a legal prohibition to which the relevant entity is subject should be treated as effective, and that the presumption of compliance may be displaced only where there is concrete evidence relating to that entity; in particular, evidence that it, or an entity in a comparable position, has breached or circumvented the same or a similar prohibition in comparable circumstances.

2.3 Contractual measures cannot substitute for technical de-identification, but should be given consideration

CIPL agrees with the stipulation in paragraph 34 of the draft Guidelines that a contractual prohibition is not a prohibition by law, and that there is a difference in kind between measures that have the ability to actually change what the data is and measures that govern what a recipient may do with it. Where a dataset remains technically re-identifiable in the recipient's hands, an agreement not to re-identify it does not change what the data is: information that is in substance pseudonymised does not become anonymous because the parties have agreed to treat it as such. Consistent with its position on Article 6(11) DMA, CIPL considers that technical de-identification should carry the decisive work of reducing identifiability, with contractual and organisational safeguards reinforcing a technically sound outcome rather than bridging a technical gap.[15]

Paragraph 34 does not address the weight those safeguards carry once the technical work has been done. Every anonymisation process relies to some degree on governance to manage residual risk, and where that risk is marginal, binding restrictions on the recipient form part of the assessment of the likelihood of identification. Paragraph 34 may be read as discounting contractual measures rather than weighing them. That reading would be difficult to reconcile with a number of established positions:

- the recipient-relative analysis in *EDPS v SRB*, which turns on the conditions actually attaching to the recipient's position;

[14]Draft Guidelines, paras. 32 and 33. The Court's position is set out in C-582/14 *Breyer*, para. 46, C-479/22 P *OC v European Commission*, para. 51, and C-413/23 P *EDPS v SRB*, para. 82, cited at footnote 28 of the draft Guidelines.
[15]CIPL, A Single Standard for Anonymisation (July 2026), Recommendation 3.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

- the GDPR's own reliance on contractual instruments in Article 28 and in the standard contractual clauses adopted under Article 46;
- binding corporate rules under Article 47, which make intra-group commitments legally binding and enforceable;
- the EDPB's Recommendations 01/2020, which treat contractual commitments as a meaningful component of a layered package of measures;[16] and
- the Joint Commission–EDPB Guidelines, on which the draft itself relies for the proposition that measures should be reliable, verifiable and enforceable.[17]

The question for the final Guidelines is therefore how much weight contractual safeguards carry, rather than whether they carry any.

The final Guidelines should distinguish between the two roles contractual measures may play. Technical measures must carry the decisive work of reducing identifiability: data which remains technically re-identifiable by its recipient is not rendered anonymous by an agreement not to re-identify it, not least because audits cannot reliably reveal whether a recipient has combined the data with its own. Where technical measures have already achieved that outcome and only marginal residual risk remains, contractual and organisational restrictions that are specific, verifiable and enforceable should be weighed in assessing whether the remaining likelihood is insignificant. CIPL would further encourage the EDPB, the Commission and national authorities to settle the balance between the technical and governance layers together, given that the same concept is being applied in parallel under the DMA.

Where technical measures have done that work, binding and enforceable commitments, backed by audit rights and meaningful sanctions, should be presumed to be honoured unless there is concrete evidence otherwise, mirroring the approach to legal prohibitions in paragraphs 32 and 33. The possibility, noted in paragraph 34, that contracts may be revised or ignored should be assessed on the evidence in the case at hand, not applied as a general discount. Common control within a corporate group should not, of itself, count as such evidence, particularly where commitments are embedded in audited group policies or binding corporate rules.

2.4 Anonymity should not require proof of a negative

A documented, reasoned assessment supported by appropriate safeguards should stand unless a concrete and reasonably likely route to re-identification is shown. Theoretical possibilities, the unknown capabilities of unidentified actors or techniques that may emerge in future should not suffice; paragraph 33 already applies a comparable evidential threshold to legal prohibitions. Accountability under Article 5(2) GDPR presupposes that data is personal and cannot settle that question. For the same reason, paragraph 47 should not present a finding of anonymity as a potential "false positive" simply because the assessor cannot know every entity's means; that framing sits uneasily with the presumption of anonymity in paragraph 95.[18]

[16]EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, para. 98.

[17]Draft Guidelines, footnote 29, citing European Commission and EDPB, Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation (version for public consultation), para. 181. See also draft Guidelines, paras. 29(b) and 90.

[18] Draft Guidelines, paras. 33, 47 and 95.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

3. The applicable perspective should not displace the GDPR's allocation of roles

The draft Guidelines provide in paragraph 15 that, where an entity processes information on behalf of another, whether the data is personal in the hands of that processing entity is assessed by reference to the controlling entity's perspective. The effect is that data which is personal for a controller cannot be anonymous for an entity processing on its behalf.[19] The GDPR relies on the concept of the processor to prevent controllers from circumventing its protections through outsourcing, and that concern is entirely legitimate. Paragraph 15 is, however, difficult to reconcile with the draft's own terminology and analytical framework. Paragraphs 4 and 5 explain that the Guidelines deliberately avoid the labels "controller" and "processor", using instead "entity" and "given data", precisely because an entity's status as controller or processor depends on whether the data at issue is personal data in its hands. Paragraph 15 appears to reverse that sequence: it characterises the receiving entity as a processor and relies on that characterisation to conclude that the data is personal data for that entity.

In doing so, it risks assuming the very conclusion that the Guidelines' assessment is intended to determine. A categorical rule is also difficult to reconcile with the contextual approach the draft otherwise adopts, and with the Court's reasoning in *EDPS v SRB* that pseudonymisation may, depending on the circumstances, effectively prevent persons other than the controller from identifying the data subject. The Court framed that analysis by reference to "another person" and did not confine it to entities determining their own purposes and means.[20] The implications are most apparent for cloud and other large-scale enterprise service providers, which often receive strictly limited datasets, are contractually and technically prevented from accessing identifying information, and have no means reasonably likely to be used to identify any individual.

The final Guidelines should allow that an entity processing on behalf of another may, in defined circumstances, be processing anonymous data. That conclusion should rest on a contextual assessment of the data actually shared, the instructions and restrictions under which it is held, the technical and organisational measures in place, and the means reasonably likely to be used by that entity.

4. Separation within an organisation should be taken into account

Many organisations operate separate, independently managed data systems. They may confine analytics and research to segregated environments that receive only de-identified data, while keys and identifying data are held elsewhere and controlled by different teams. The draft does not address this, although paragraphs 10 and 12 contemplate anonymisation without deletion and for an entity's own use. CIPL recognises that an entity is a legal person and that, under Article 4(5) and Recital 26 GDPR, pseudonymised data remains personal for whoever can attribute it. Effective internal separation, through technical segregation, access controls, separation of duties, monitoring and enforceable internal rules, is nonetheless an objective factor bearing on the means reasonably likely to be used, much like the access restrictions in paragraphs 89 and 90.[21]

The final Guidelines should clarify whether, and on what conditions, such separation can make data anonymous within the ring-fenced environment, and illustrate this with a worked example. This would

[19] Draft Guidelines, para. 15: "In practice, this means that if an entity processes information on behalf of a controller (*i.e.* someone for whom the information is personal data, and who decides the purposes and means of the processing), that information should also be considered personal data for the processing entity".
[20] C-413/23 P *EDPS v SRB*, paras. 79 and 87.
[21] Draft Guidelines, paras. 10, 12, 89 and 90; Article 4(5) and Recital 26 GDPR.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

further encourage investment in privacy-enhancing technologies for internal as well as external uses of data.

5. The simplified approach should be positioned expressly as optional

CIPL welcomes the availability of a simplified approach, and the draft's clear statement that it does not represent an alternative legal standard. The combined use of the two approaches described in paragraph 49 is of practical value and reflects the way many organisations already work.

CIPL's concern lies in how the simplified approach may come to operate in practice. Because it is more straightforward to apply, is described in the draft as providing greater confidence, and carries the authority of EDPB guidance, it may in time be treated as the expected course rather than as one of two available routes. Organisations may then hesitate to move to a contextual assessment, on the view that the simplified approach offers greater legal certainty. That tendency is reinforced when the safeguards distinguishing the two approaches are not given equal prominence. The statement that the simplified approach cannot be relied upon by third parties to establish that information is personal data presently appears only in a footnote.[22]

CIPL would encourage the EDPB to set out in the text, rather than in a footnote, the points that keep the two approaches properly distinguished: that the contextual approach reflects the legal standard under Article 4(1) and Recital 26 GDPR as well as the case law; that the simplified approach is an optional operational tool which, as paragraph 48 acknowledges, may provide a more cautious level of protection than is strictly necessary; that its use gives rise to no presumption that the information is personal data; and that a controller may move from the simplified approach to a documented contextual assessment at any stage, without adverse inference.

The draft Guidelines are also not sufficiently clear about what the simplified approach tests: theoretical possibility (paragraph 49), or means reasonably likely to be used by at least someone (paragraphs 100 and 103), setting aside differences between entities (paragraphs 45 and 48).[23] The final Guidelines should say which. If it is the former, the approach departs further from the legal standard, and an adverse result cannot establish that data is personal. Paragraph 96, which refers to data "found to be personal under the simplified approach", should instead state that anonymity has not been demonstrated under that approach.

6. The No Inference criterion should be more clearly defined

CIPL welcomes the inclusion of inference as a criterion. The definition in paragraph 67, requiring that an inference be both specific and meaningful, is the correct conceptual approach, and Examples 13 and 14 usefully exclude generalisation from the population at large.

However, that inference boundary is currently not sufficiently clearly drawn. The discussion at paragraphs 76 to 82, particularly on de-aggregation, AI models and synthetic data, is broad enough to leave organisations uncertain whether ordinary analytics, published statistics, synthetic datasets and trained models fall within the criterion whenever they might, in combination with other information, reveal something about an individual. Read expansively, the criterion would treat as personal data a wide range of outputs from which no individual is in fact reasonably likely to be identified. That

[22] Draft Guidelines, footnote 36.
[23] Draft Guidelines, paras. 45, 48, 49, 96, 100 and 103.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

outcome is difficult to reconcile with the draft's own emphasis on realistic likelihood and with the EDPB's more calibrated treatment of AI models in Opinion 28/2024.[24]

The EDPB should draw that boundary more explicitly in two ways. First, the Guidelines should reaffirm that generalisation, meaning a pattern that holds across a population and applies equally to individuals who were never in the original dataset, does not violate the criterion, consistent with Example 14. Second, the treatment of AI models should be aligned with Opinion 28/2024, so that the question is whether personal data can be extracted from or regurgitated by the model with means reasonably likely to be used, rather than whether the model is capable of producing statements about people. Measurable indicators, such as differential privacy parameters or disclosure-risk testing, can support that assessment and should be recognised, without any single metric being mandated.

7. Singling out should be defined and distinguished from identification

Singling out carries considerable weight in the draft Guidelines. It is introduced through the No Record Isolation criterion at paragraph 54, and paragraph 98 makes it the test that determines whether a dataset failing that criterion is nevertheless anonymous. The term is not, however, defined. Footnote 37 indicates that the concept will be explained in detail in section 3.5.3, but paragraph 98 describes how singling out may be carried out rather than setting out what it means.

The relationship between paragraph 98 and paragraph 19 would also benefit from clarification. Paragraph 19 treats a person as identified where they can be distinguished within a given context so as to make it possible to treat them differently. Paragraph 98 concludes that an individual who can be singled out by matching an isolated record to their corresponding attributes should be considered identifiable, without reference to that second element. Example 24 indicates that the element is material: the survey data is regarded as anonymous despite unique records because there is no way to link the answers to a respondent's identity, "nor to treat any respondent differently based on their individual answers". The example therefore applies a fuller test than the one set out in paragraph 98.[25]

CIPL would encourage the EDPB to define singling out in the Guidelines, and to align paragraph 98 with paragraph 19 and with the reasoning in Example 24, so that an individual is treated as identifiable only where a relevant entity can both attach the isolated record to that individual, using means reasonably likely to be used, and treat them differently as a result.

8. The Guidelines should map common techniques and PETs to the three criteria

Opinion 05/2014 provided a technique-by-technique account of aggregation, generalisation, noise addition, permutation, k-anonymity, l-diversity and differential privacy, setting out for each its strengths, its limitations and its common failure modes.[26] The draft replaces that treatment with three criteria of general application. The criteria are a better analytical framework, but the practical layer has not been carried forward. Organisations that have invested in privacy-enhancing technologies (PETs) are therefore left without guidance on how those measures are to be evaluated under the draft Guidelines. This is a matter of adoption as much as of compliance. CIPL's research on PETs highlighted

[24]EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, paras. 31–35 and 39–43.
[25]Draft Guidelines, para. 98 and Example 24; see also para. 54 and footnote 37.
[26]Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

that uncertainty about their legal effect is among the most significant obstacles to their deployment, and that regulatory clarity is correspondingly among the strongest incentives to invest in them.[27]

The final Guidelines should include an annex mapping common techniques to the three criteria, or at a minimum a commitment to follow-up guidance within a defined timeframe. This should cover the techniques addressed in Opinion 05/2014 as well as newer approaches such as differential privacy, synthetic data generation, federated learning, secure multi-party computation and trusted execution environments. For each, the guidance should explain which criteria it typically addresses, where it typically fails, and which parameters or deployment conditions determine the outcome. Such guidance should not mandate any particular technology; PETs are one of a range of routes to the desired outcome, and the assessment should remain focused on the result achieved.

9. The legal basis for anonymisation should follow the activity it serves

Paragraph 38 presumes that anonymisation shares the legal basis, and any Article 9(2) exemption, of the preceding processing where it forms part of the same activity and serves the same purposes. CIPL welcomes the effort to ease the possibility of anonymisation. In practice, however, anonymisation is often applied to datasets that combine several collections, purposes and legal bases, precisely in order to reduce privacy risks. Read narrowly, paragraph 38 would make the step that most reduces risk to individuals harder to justify than continued processing of identifiable data.

The EDPB's own guidance points the other way. The legal basis for processing extends to the operations needed to pseudonymise the data;[28] anonymisation is recognised as an alternative to deletion under data protection by design;[29] and Opinion 05/2014 treated anonymisation that reliably produces anonymous data as compatible further processing.[30] The draft Guidelines on processing for scientific research purposes are more hesitant about anonymisation than about pseudonymisation.[31] Paragraph 39 of the draft itself treats anonymisation as a safeguard within the preceding processing, and the GDPR treats pseudonymisation and encryption as safeguards in Articles 6(4)(e) and 32(1)(a). Anonymisation should not be the only measure of this kind to require separate justification.

The final Guidelines should confirm that the presumption is not exhaustive and that anonymisation is covered by the legal basis of the activity it serves, including where it is carried out for data minimisation, storage limitation or data protection by design. Using the anonymous output for a different purpose should not in itself call for a new legal basis for the anonymising step, so long as the existing basis remains appropriate and the further use is compatible under Article 6(4) GDPR. A worked example, including a consolidated dataset, would help.

10. The terms "de-identified" and "de-personalised" should not be treated as equivalent to "anonymous"

CIPL supports the objective of paragraph 40 of the draft Guidelines, that controllers should not describe data as anonymous where individuals remain identifiable, and precision in transparency information is important.

---

[27] CIPL, Understanding Privacy Enhancing Technologies and Privacy Preserving Techniques (December 2023).
[28] EDPB, Guidelines 01/2025 on Pseudonymisation (version for public consultation), para. 23.
[29] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, paras. 53–54 and 75.
[30] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, section 2.2.1.
[31] EDPB, Guidelines 1/2026 on processing of personal data for scientific research purposes (version for public consultation), paras. 156 and 158.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Paragraph 40 lists "anonymous", "de-identified" and "de-personalised" together, which may suggest that the three are equivalent. In practice, and particularly in AI contexts, the terms are often used interchangeably although they carry different meanings. "Anonymous" expresses a legal conclusion, namely that the data falls outside the scope of the GDPR. "De-identified" and "de-personalised" are generally used to describe data to which de-identifying measures have been applied but which may remain personal data, and which is closer in substance to pseudonymised data. Under a number of US state privacy laws, "deidentified" is a defined term for data that, subject to conditions, falls outside their scope,[32] and global organisations use it in that sense.

CIPL would encourage the EDPB to be clear that "de-identified" and "de-personalised" may continue to be used to describe data that is not considered anonymous in the sense of the GDPR. The prohibition in paragraph 40 would then attach to misleading claims that the GDPR no longer applies, while organisations retain the vocabulary needed to describe intermediate states of identifiability accurately.

11. Documentation and reassessment should be proportionate and linked to concrete external factors

CIPL supports the accountability framing of paragraphs 41 and 42. Documentation of the anonymisation process, including the testing of supposedly anonymous datasets, is the evidence that allows organisations to demonstrate their reasoning to supervisory authorities. Periodic reassessment is also a sound approach, since identifiability risk changes as techniques improve and auxiliary data becomes available. Paragraph 35 frames reassessment as good practice, to be undertaken wherever possible and as appropriate, and footnote 3 confirms that assessments made under Opinion 05/2014 need not be repeated. The draft does not, however, give content to what is appropriate, or any sense of proportion as to the form, depth, frequency or endpoint of the exercise. Read together with paragraph 42 on security incidents and paragraph 88 on safety margins, that open-ended framing could absorb considerable resources on large-scale or long-retained datasets without a corresponding benefit to individuals. That is particularly so where the data has been aggregated and the original dataset deleted, so that little can be done in response to a review beyond recording that it has taken place.

The final Guidelines should set risk-tiered documentation expectations, calibrated to the sensitivity of the data, the number of individuals concerned and the breadth of access, together with a model assessment record structured around the three criteria. Reassessment should be triggered by material change, such as broader access or release, newly available linkage data, a relevant security incident, a change in technique, or a demonstrated advance in re-identification capability. For higher-risk datasets, this could be supplemented by a proportionate periodic review. CIPL would also welcome confirmation, consistent with footnote 3 of the draft, that assessments carried out in good faith continue to be recognised unless the facts materially change.[33]

12. Several examples should be developed further

- **Example 3** concludes that the agency must treat the records as personal data because the retailer is able to identify the customers, but does not indicate which excerpts the agency receives, whether it can access the retailer's identifying information, or what restrictions apply to it.

[32] See, for example, California Civil Code § 1798.140(m).
[33] Draft Guidelines, footnote 3.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

- **Example 7** proceeds on the basis that the business partner "could easily hire" a third party to perform re-identification, without offering a benchmark for when an outsourced capability is realistically available, or addressing the safeguards that may make such an engagement unlikely.
- **Example 9** stops at the point at which the analysis would become most helpful. It does not specify the datasets or matching method, identify the relevant entities and the scope of their access, or carry either approach through to a conclusion, and therefore does not show whether the two produce different outcomes.
- **Example 18** states that membership can be inferred, but does not identify the attributes, the technique, the auxiliary information required, or the basis on which the result would be reliable enough to distinguish Alex from others.
- **Example 20** does not explain how the entity would know that one inference is correct without knowing to whom it relates, nor what "significant confidence" and "reasonable precision" are intended to mean in operational terms.

For each major topic, the EDPB should develop at least one example into a worked analysis. Such an analysis would identify the relevant entity and dataset, describe the concrete isolation, linkage or inference pathway, state the access conditions and operative safeguards, supply any necessary qualitative or quantitative threshold, apply the legal standard step by step, and include a paired counterfactual identifying the single fact that changes the result. This would enable organisations to reproduce the reasoning rather than simply adopt the conclusion.

The final Guidelines should also include examples in which anonymisation succeeds, each explaining why the residual likelihood of identification is insignificant. Candidates include aggregated commercial analytics, fraud-prevention models, pseudonymised data shared while the key stays with the disclosing entity, and granular datasets used in research, health and mobility.

13. AI model training, synthetic data and model evaluation should be addressed directly

The draft refers to AI models and synthetic data at paragraphs 77 and 82 and cites Opinion 28/2024, but it contains no example or sustained analysis of how the framework applies to model training, synthetic data generation or model evaluation. These are among the anonymisation questions that arise most frequently in practice, and they are precisely the contexts in which organisations are being encouraged to adopt privacy-preserving alternatives to processing personal data at scale.

The EDPB should provide practical guidance and at least one worked example on each of these questions. The guidance should address whether and when data used for model training and evaluation can be treated as anonymous, and from whose perspective. It should also address the conditions under which synthetic data may be regarded as anonymous, and the generation parameters and evaluation methods that bear on that conclusion. Finally, it should explain how the three criteria apply to a trained model, consistent with Opinion 28/2024. Without such guidance, organisations will face the greatest regulatory uncertainty precisely where privacy-preserving approaches hold the most promise, an outcome that serves neither responsible innovation nor the individuals the framework is designed to protect.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Summary of recommendations

In the context of the EDPB draft Guidelines 02/2026, CIPL respectfully recommends that the EDPB:

1. **Ensure coordination across parallel processes in which the same concept of anonymisation is being determined.** The anonymisation standard set in the GDPR should remain the governing standard wherever "anonymised" appears in EU law. Work with the Commission and national authorities so that the same standard is applied consistently and coherently in the DMA and other Union law; and commit to reviewing the Guidelines once the Digital Omnibus has concluded.
2. **Draw the two directions of the likelihood assessment together.** Set out, alongside the factors in paragraph 29, the considerations that reduce realistic identifiability, and explain how the two are to be weighed.
3. **Anchor the assessment in concrete rather than conceivable means.** Direct the analysis to means that are real or reasonably foreseeable in the circumstances, particularly where the data is not made publicly available. Do not let the general statements on cost and AI in paragraphs 92 and 93 pre-empt the assessment of effort.
4. **Align the burden in paragraph 21 with the standard in paragraph 22.** Ask whether identification by the recipient is reasonably likely, rather than whether it can be ruled out.
5. **Distinguish capability from likelihood.** The possibility that a key-holder could disclose a key held under Article 4(5) GDPR should not, by itself, make pseudonymised data personal for the recipient, including within a corporate group.
6. **Bring the qualification in paragraph 30 into the operative text.** Confirm that unauthorised and accidental access are relevant where the facts show a realistic likelihood of both access and successful re-identification, as Example 22 illustrates. Where the security controls in paragraph 89 apply, treat unauthorised actors as relevant only on concrete evidence.
7. **Align the grounds in paragraph 33 with that paragraph's own test.** Confine them to evidence relating to the entities involved, rather than to general propositions about legal systems or hypothetical actors.
8. **Distinguish the two roles of contractual measures.** Confirm that technical measures carry the decisive work of reducing identifiability, and that specific, verifiable and enforceable safeguards with meaningful consequences for breach are duly weighed once that work is done. At that point, presume binding commitments are honoured, absent concrete evidence to the contrary.
9. **Do not require proof of a negative.** A documented, reasoned assessment should stand unless a concrete, reasonably likely route to re-identification is shown; align paragraph 47 with paragraph 95.
10. **Allow for anonymity in the hands of a processing entity.** Recognise that an entity processing on behalf of another may, in defined circumstances, process only anonymous data, consistent with the contextual approach and with *EDPS v SRB*.
11. **Take separation within an organisation into account.** Clarify whether and when data in a ring-fenced environment can be anonymous, with a worked example.
12. **Position the simplified approach expressly as optional.** State in the operative text that the contextual approach reflects the legal standard, that use of the simplified approach creates no presumption that data is personal, and that organisations may move between the two without adverse inference. Clarify what the simplified approach tests.
13. **Bound the No Inference criterion.** Distinguish inferences about an identifiable individual from population-level generalisation, and align the treatment of AI models with Opinion 28/2024.
14. **Define singling out, and distinguish it from identification.** Align paragraph 98 with paragraph 19 and with the reasoning in Example 24, so that identifiability requires both that

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

an isolated record can be attached to a particular individual and that the individual can be treated differently as a result.

15. **Map common techniques and privacy-enhancing technologies to the three criteria.** Carry forward the practical layer of Opinion 05/2014 in an annex or in prompt follow-up guidance.
16. **Align the legal basis for anonymisation with the activity it serves.** Treat paragraph 38 as non-exhaustive and address different downstream uses and consolidated datasets.
17. **Keep "de-identified" and "de-personalised" distinct from "anonymous".** Clarify the distinction, and confirm that those terms may continue to be used to describe data that remains within the scope of the GDPR.
18. **Calibrate documentation and reassessment to risk.** Give content to what is appropriate under paragraph 35, through risk-tiered expectations, a model assessment record and change-based triggers.
19. **Develop key examples into worked analyses.** Supply the facts that Examples 3, 7, 9, 18 and 20 omit, and carry at least one example under each major topic through to a reasoned conclusion. Include examples in which anonymisation succeeds.
20. **Address AI model training, synthetic data and model evaluation directly.** Provide practical guidance and at least one worked example on each, consistent with Opinion 28/2024.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.