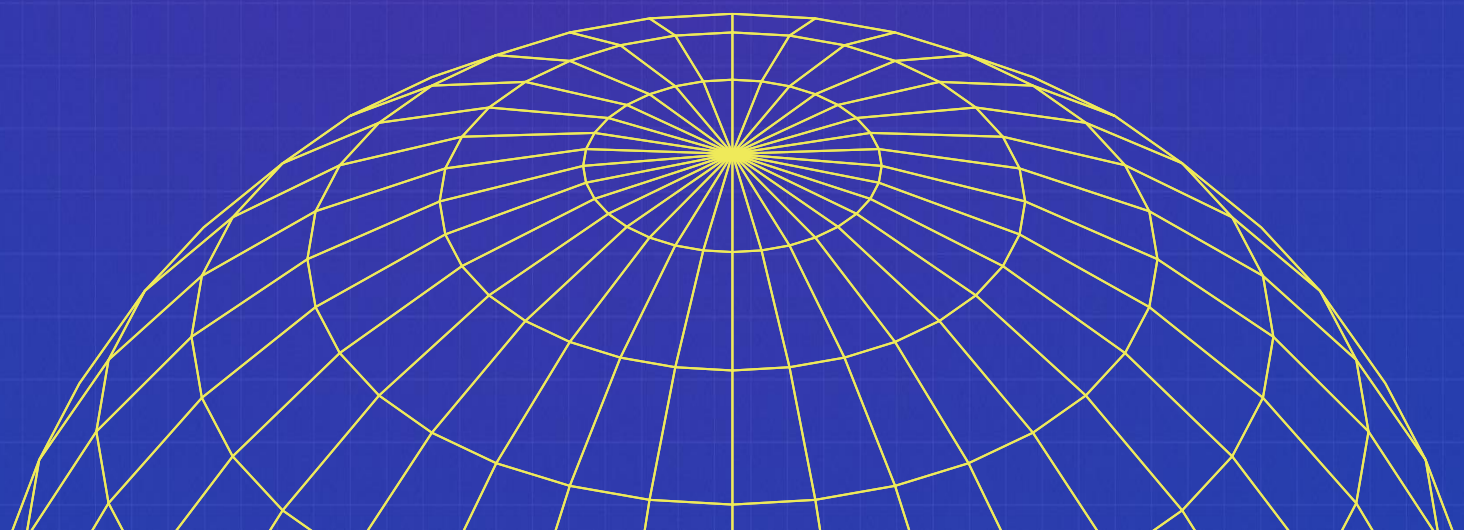
DOT. europe

October 2026

DOT EUROPE RESPONSE TO CONSULTATION

DOT Europe contribution to the EDPB consultation on Guidelines 02/2026 on Anonymisation



DOT Europe contribution to the EDPB consultation on Guidelines 02/2026 on Anonymisation

1. Introduction

DOT Europe welcomes the opportunity to comment on the EDPB draft Guidelines 02/2026 on Anonymisation (the "draft Guidelines").[1] Clear and workable guidance on anonymisation directly supports the objectives of the GDPR, including data protection by design (Article 25).

The draft Guidelines rightly update Opinion 05/2014 and adopt the entity-relative approach confirmed by the CJEU in *EDPS v SRB*.[2] In several places, however, they set a threshold closer to impossibility than to the "means reasonably likely to be used" standard of Recital 26. Setting an unrealistically high bar for anonymisation brings privacy-protective processing back within the full GDPR regime without a matching gain in protection for individuals.. The draft Guidelines also contain internal inconsistencies and offer few examples of anonymisation that succeeds. As drafted, few analytically useful datasets could qualify as anonymous, which would discourage investment in de-identification and privacy-enhancing technologies. This contradicts broader EU policy initiatives aimed at regulatory simplification and digital competitiveness. Our comments propose targeted changes to make the EDPB framework helpful in practice and better aligned with the commitments to clearer and more practical guidance made in the EDPB's Helsinki Statement and its 2024-2027 Strategy.[3]

2. Points we support

DOT Europe particularly welcomes the following elements of the draft Guidelines:

- **Entity-relative approach (paras 6 - 7 and 11 - 12).** The recognition that data may be anonymous for some entities but not for others, and that the relevant perspective depends on for whom the data is intended to be anonymous.
- **Insignificant risk, not zero risk (paras 8 and 22).** The confirmation that identifiability is a question of likelihood, and that the likelihood of identification must be insignificant in reality rather than zero.

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

[2] CJEU, C-413/23 P, *EDPS v SRB*, 4 September 2025, ECLI:EU:C:2025:645.

[3] EDPB, The Helsinki Statement on enhanced clarity, support and engagement, 3 July 2025. See also EDPB, Strategy 2024-2027, adopted in April 2024, and EDPB, Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation, Fostering Cross-Regulatory Consistency and Cooperation, 3 December 2024

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

- **Objective factors (para 29).** The list of factors relevant to the means reasonably likely to be used, including context, access restrictions, the cost and time of obtaining additional information, and available technology.
- **Legal prohibitions and security controls (paras 32 and 89).** The general assumption that people follow the law, and the statement that, where data is subject to appropriate security controls, access is a means reasonably likely to be used only by authorised users.
- **Anonymisation without deletion and continuity (para 10 and footnote 3).** The recognition that anonymisation does not require deletion of the original data, and that assessments carried out under Opinion 05/2014 need not be repeated.
- **Legal basis and legitimate interest (paras 38 - 39).** The presumption that the legal basis for anonymisation coincides with that of the preceding processing, and the recognition of anonymisation as a positive factor in the legitimate interest balancing test. It is, however, important that the Guidelines confirm that anonymisation carried out to enhance privacy or conduct secondary business analytics is compatible with initial collection purposes under Article 6(4) GDPR (see section 4.5).
- **Population-level inferences (paras 69 - 71 and Examples 13 - 14).** The distinction between inferences drawn from population-level information and inferences that rely on an individual's data, and the practical test in para 71(b), which compares outputs produced with and without an individual's records.
- **Limits of the simplified approach (footnote 36).** The clarification that the simplified approach cannot be used by third parties to prove that data is personal.

3. Overarching principle: a realistic, evidence-based assessment of re-identification risk

Recital 26 GDPR and CJEU case law set a standard of reasonableness. Identification must be reasonably likely, taking into account all objective factors and the technology available at the time of processing, and the risk must be insignificant "in reality" rather than excluded in theory.[4] The draft Guidelines state this standard correctly in paras 8, 22 and 29. Elsewhere, however, they replace it with tests asking whether identification "cannot be ruled out" or could conceivably occur in the future (paras 21, 30, 31, 35 and 92). A test that can never be passed removes the incentive to anonymise, or even attempt it.

We therefore invite the EDPB to apply three principles throughout the final Guidelines:

- **Foreseeable, not conceivable.** Actors, means and future events should count where the facts show a realistic pathway to access and successful re-identification, not merely because they are possible. The assessment should focus on actual and foreseeable recipients and the means reasonably likely to be used by them, extending to actors only where the facts show a realistic pathway to the data.

[4] CJEU, C-582/14, *Breyer*, 19 October 2016, ECLI:EU:C:2016:779, para 46; *EDPS v SRB*, para 82.

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

- **All factors count, in both directions.** The assessment should weigh together the factors that increase identifiability (auxiliary data, access, capability) and those that reduce it (cost, time, expertise, security controls, legal and contractual constraints, other safeguards).
- **Outcome-based and technology neutral.** The Guidelines should state the result required and leave the means open, recognising that different combinations of technical, organisational and contractual measures can achieve it.

This would give controllers a target they can meet and document, and give supervisory authorities a consistent benchmark.

4. Specific concerns and recommendations

4.1 Relevant entities and unauthorised actors

- **"Cannot be ruled out" (para 21).** Read literally, para 21 suggests that if an entity transfers data to a recipient who might transfer it to a party capable of re-identification, the data would become personal data for the original transferring entity. This would expose data originators sharing data without any re-identification key to open-ended liability if a downstream recipient subsequently suffers a breach or improperly transfers data to an adversarial party. The 'cannot be ruled out' wording also sets an impossibility threshold. The case law cited concerns an actual transfer to an actual recipient with means reasonably likely to be used.[5] We suggest referring instead to cases where "it is reasonably likely that the receiving entity has the means" to identify the individual. The Guidelines should also clarify that the transferring entity's assessment is made on the basis of the means reasonably foreseeable at the time of transfer, so that unauthorised downstream actions do not retroactively change the status of the original transfer. This is without prejudice to forward-looking reassessment where a material change occurs (see section 4.2).
- **Unauthorised and malicious actors (para 30 and Example 22).** Para 30 lists rogue employees, cybercriminals, unethical companies and foreign intelligence agencies among the relevant entities. Read in isolation, this list suggests that trusted recipients must be assessed against the same worst-case standard as adversarial actors. Footnote 25 rightly notes that they need not be considered systematically, and para 89 states that, with appropriate security controls, access is a means reasonably likely to be used only by authorised users. The main text, in particular para. 30 and following should reflect this: such actors should be considered where the facts show a realistic pathway, such as weak security, prior incidents or public release, as in Example 8.[6] Example 22, which treats hacking and accidental disclosure as reasonably likely despite state-of-the-art security, should be revised accordingly.

[5] *Breyer*, paras 47–49; CJEU, C-319/22, *Scania*, 9 November 2023, ECLI:EU:C:2023:837, paras 45–49; *EDPS v SRB*, paras 84–85.

[6] This is consistent with stakeholder feedback summarised in EDPB, Report on the stakeholder event on anonymisation and pseudonymisation, section 3, which called for unlawful means to be assessed by reference to objective factors such as foreseeability, realistic access pathways, the availability of auxiliary data and applicable safeguards.

Avenue Marnix, 17
1000 Brussels,
BELGIUM
TEL +32 (0)472 26 83 02
MAIL info@doteurope.eu
WEBSITE www.doteurope.eu

- **Proportionate to the sharing environment.** Threat modelling should scale with the openness of the environment. Assuming that a vetted partner working in a secure, contractually controlled environment will behave like a malicious hacker is disproportionate, whereas broad public release justifies a wider threat model. The same reasoning applies to intra-group and affiliate recipients: where they receive aggregated or tokenised data under documented technical and contractual access controls, they should be treated as a distinct, lower-risk category rather than assessed against the standard applied to adversarial third parties.
- **Access as a threshold (para 9 and footnote 21).** The draft Guidelines already provide the basis for a proportionate threat model. Para 9 states that an entity which cannot access the data, is not meaningfully connected to an entity with access, and is not likely to receive the data need not be assessed. Footnote 21 adds that the likelihood of transfer or access is considered from the point at which the entity for which the data is intended to be anonymous receives it. The final Guidelines should make this the explicit first step of the para 30 analysis: an actor should be relevant only where there is a realistic pathway by which it could obtain the data, judged against the security and access controls in place.
- **Accident, negligence and motivation (para 31).** Accidental or negligent identification should matter only where it is reasonably foreseeable in the circumstances; these risks are primarily addressed through security obligations under Article 32 GDPR. Lack of motivation should not be decisive on its own, but it should remain a relevant factor alongside capability, cost and time, as para 31 already accepts for the value of re-identified data and the risks for the re-identifying entity.
- **Compelled disclosure.** Likewise, the scenario of an entity "forced by outside circumstances" to identify individuals or transfer data should be assessed on concrete evidence of a realistic pathway, consistent with para 33. Such compulsion is relevant only where the compelled entity holds, or could obtain, the means of re-identification. The existence of third-country access laws should not by itself defeat anonymity.
- **Outsourced capabilities (Example 7).** Treating the mere possibility of hiring a third party as sufficient goes beyond the "reasonably likely" standard set by the GDPR and the CJEU. The example should explain when hiring a third party to re-identify data is realistically available, and take into account safeguards, such as contractual prohibitions, that would deter it.

4.2 Time, cost and the evolution of risk

- **"Impossible in practice" (para 26).** The CJEU refers to identification that is "practically impossible" or "impossible in practice". Para 26 drops this qualifier, which changes the meaning of the test. It should be restored.
- **Time and cost (paras 26, 29(d) and 92).** Para 92 states that time and cost would generally not be prohibitive, which sits uneasily with paras 26 and 29(d), where they are core factors. Para 92 should be reframed as a factor to be assessed case by case. It should also be clear that an entity's greater resources or AI capabilities do not in themselves defeat anonymity; otherwise the organisations best able to invest in anonymisation could never achieve it.
- **Foreseeable technology and AI-driven means (paras 29(d) and 29(e)).** The reference to "reasonably foreseeable technological developments" should be anchored to techniques demonstrated in the state of the art at the time of the assessment, such as published and

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

reproducible attacks, and to means realistically available to the relevant entity. The Guidelines should also explain how AI-driven reductions in the time and effort needed to combine sources feed into this assessment, with criteria or examples distinguishing existing from hypothetical means that can be revisited as the technology develops. Speculative future capabilities should be handled through the reassessment triggers set out below, not by treating data as personal data today. Otherwise, para 29(e) would reintroduce the "conceivable" test that section 3 cautions against.

- **Reassessment (paras 35, 42 and 88).** Periodic review is good practice, but an open-ended duty, without operational triggers implies that no dataset is ever conclusively anonymous. The Guidelines should set clear criteria for when reassessment is required: it should be triggered by material changes, such as wider access, newly available linkage data, a security incident affecting a safeguard relied upon or a demonstrated advance in re-identification capability,with any periodic review following a proportionate, risk-based cycle. . The safety margins in para 88 should likewise be proportionate to the risk.
- **Documentation (para 41).** We support documenting anonymisation assessments. Risk-tiered expectations and a model assessment record structured around the three criteria would help controllers apply this consistently. Lineage records showing the source data, the techniques applied, the assessment relied on and the recipients should be accepted as meeting para 41 and as the basis for targeted reassessment.

4.3 Contractual and organisational measures

DOT Europe agrees that strong technical measures should remain the primary safeguard, and that contracts alone do not change the nature of data and cannot replace technical measures. Para 34 rightly requires measures to be reliable, verifiable and enforceable, but it then states that contractual prohibitions “should not be treated as a prohibition by law” and may "even be disregarded entirely". Para 90 adds that such measures are not by themselves sufficient.

Giving contractual safeguards little weight sits uneasily with Recital 26, which requires all objective factors to be taken into account. Binding contractual obligations are enforceable in court and backed by consequences such as damages, termination and regulatory exposure: exactly the "risks that re-identification entails" that para 31 considers relevant. The GDPR itself relies on contracts as safeguards (Articles 28 and 46(2)(c)), and EU data access regimes rest on enforceable commitments not to re-identify.[7]

We recommend replacing the categorical approach in para 34 with an evidential test, , applying to contractual prohibitions the same approach that para 33 applies to legal prohibitions. A prohibition on re-identification that is specific, legally binding, verifiable (for example through audit or technical attestation) and backed by enforceable consequences should, together with technical and organisational measures, be presumed to reduce the means reasonably likely to be

[7]See, for example, Article 40 of Regulation (EU) 2022/2065 (Digital Services Act) on data access for vetted researchers, and Article 61(3) of Regulation (EU) 2025/327 (European Health Data Space) on the obligations of health data users.

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

used. Evidence of the kind para 33 lists, such as prior breaches or absent monitoring, can rebut that presumption. The bare possibility of non-observance should not disqualify a measure, since any measure, including encryption or access controls, may fail if misapplied.

A contractual restriction should not, by itself, establish anonymity. It may nevertheless be relevant to whether identification is reasonably likely where it is binding, enforceable and supported by evidence of implementation, for example access controls, audit rights, meaningful consequences for breaches (including disciplinary consequences for rogue employees) and the ability to suspend or terminate access. Its weight should be assessed alongside the technical and organisational safeguards and the recipient's actual access and capabilities.

4.4 Anonymisation within an organisation and by processors

- **Intra-organisation anonymisation (paras 5, 10 and 12).** Para 10 accepts anonymisation without deletion, and para 12 recognises that an entity's own use can be the relevant perspective. Yet the worked illustrations either concern external disclosure (Example 8) or couple anonymisation with deletion of the source data (Example 22 and paras 39 and 71(c)). The EDPB should confirm that data can be anonymous within a ring-fenced environment, for example a dedicated team working only with anonymised outputs, even where source data is retained elsewhere in the organisation, provided re-identification is not reasonably likely from that internal perspective. A worked example addressing how this fits with the perspective of the legal entity as a whole, and distinguishing a policy-based silo from a genuine barrier to re-identification (such as separated keys, restricted access to source data and no realistic route to recombine the output with identifiable records), would help. This would encourage organisations to anonymise data for internal use, in line with data minimisation (Article 5(1)(c)) and data protection by design (Article 25).
- **Processors (para 15 and Example 3).** Para 15 implies that data which is personal for a controller is always personal for its processor. We understand the anti-avoidance rationale, but the entity-relative approach in paras 9 and 22 should still apply. Where a processor receives only a minimised dataset, has no access to keys or additional information, and is barred technically and contractually from re-identification, the data should be capable of being anonymous from its perspective. The controller's obligations would be unaffected, as para 37 confirms. At a minimum, the Guidelines should confirm two things: (i) processor obligations under the provisions listed in footnote 12 apply in proportion to the risk, given that the processor cannot identify individuals; and (ii) where a provider processes data it receives for its own purposes, its own perspective applies, as in Example 4. Example 3 should specify what data is shared, what other information the processor can access and which safeguards apply. This matters in particular for cloud and enterprise services. The Guidelines should also clarify how the assessment applies across successive processing stages. Data may remain personal during collection and transformation, while a resulting dataset may be anonymous for a recipient, depending on that recipient's role, perspective, access and realistic ability to identify individuals. The assessment of the recipient's use should not alter the status of, or the obligations applicable to, the earlier processing. A worked example should distinguish a processor acting on instructions from an independent recipient using transformed outputs.

4.5 Simplified approach, mixed datasets and legal certainty

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

- **Simplified approach (paras 47 - 49).** The final Guidelines should state clearly in the main text that the contextual approach is the legal test, that the simplified approach is an optional screening tool, and that moving from one to the other creates no adverse inference, building on footnote 36. Describing conclusions under the contextual approach as a risk of "false positives" (para 47) suggests a presumption that data is personal and should be reworded neutrally.
- **Consistent outcome (executive summary, paras 52 and 95).** Data meeting the three criteria "can be safely considered anonymous" in the executive summary, "may be regarded as anonymous" in para 52 and "can be presumed anonymous" in para 95. The Guidelines should state that where the criteria are met the data is presumed anonymous, using the wording of para 95 consistently throughout. Where an organisation has documented a reasoned assessment and implemented safeguards, a supervisory authority taking a different view should be expected to identify a concrete re-identification pathway rather than a theoretical possibility.
- **Mixed datasets (para 36).** Para 36 treats a whole dataset as personal where its parts "are not treated separately". The judgment relies on whether separation was possible within data that was already personal.[8] For enterprise platforms operating complex, distributed IT architectures across multiple teams, anonymising every record across very large datasets to the same standard is rarely achievable. Treating an entire dataset as personal because of a single vulnerable record would make compliance unworkable. We recommend assessing whether the overall risk is insignificant and recognising the detection and removal or separate handling of outlier records as a valid remediation step, so that a few outliers do not make a large dataset personal in its entirety. Documented data lineage, with technical separation of the anonymised and personal parts (for example separate storage or access-controlled partitions), should be recognised as a means of showing that the parts are treated separately.**Compatibility of anonymisation (paras 38 - 39).** Building on the presumption in paras 38 - 39, the Guidelines should confirm that anonymising personal data to enhance privacy, including to enable subsequent analytics on the anonymised data, should generally be considered compatible with the purposes of the initial collection under Article 6(4) GDPR, given that it reduces the risks for data subjects.

4.6 No Inference, AI models and privacy-enhancing technologies

- **Individuals versus populations (paras 66 - 72 and 82).** Treating AI model weights or synthetic outputs as personal data on the basis of a merely theoretical risk of membership inference would create significant barriers to machine learning, privacy-enhancing technologies and internal AI innovation. Building on Examples 13 and 14, the Guidelines should clarify the boundary between inferences about an identifiable individual and statistical patterns, model generalisation or synthetic data outputs that reflect a population. More specifically, the Guidelines should include indicative, non-exclusive criteria under which AI models and synthetic datasets can be presumed anonymous, for example where testing shows that neither individual training records nor membership of the training set can be inferred with more than insignificant likelihood using the means reasonably likely to be

[8] CJEU, C-252/21, *Meta Platforms v Bundeskartellamt*, 4 July 2023, ECLI:EU:C:2023:537, para 89.

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

used. Para 82 should be applied consistently with the case-by-case approach of Opinion 28/2024 on AI models.[9]

- **Attack techniques (paras 76 - 82 and 92; Examples 18 and 20).** Membership inference, extraction and de-aggregation are legitimate concerns, and many are the tests responsible controllers use to measure residual risk. They should be assessed against the "means reasonably likely to be used" threshold rather than treated as an automatic failure of the No Inference criterion in line with the outcome-based and technology-neutral approach set out in section 3. Examples 18 and 20 should specify the technique, the attributes used and the confidence level required to distinguish an individual.
- **Privacy-enhancing technologies (paras 90 - 91).** Beyond encryption, the Guidelines do not address PETs. Opinion 05/2014 assessed individual techniques against its criteria.[10] The final Guidelines should do the same for established and newer techniques, such as aggregation, generalisation, differential privacy, trusted execution environments, secure multi-party computation, federated learning and synthetic data, and recognise them as effective measures when properly implemented. Worked examples on AI model training, evaluation and synthetic data would be particularly valuable.

4.7 Practical guidance and examples

- **Positive worked examples.** Only a few examples reach a positive conclusion (Examples 22 and 24), and in narrow settings. The final Guidelines should include several examples where anonymisation succeeds, across contexts such as aggregated analytics, market insights, health research and mobility data, including high-dimensional records. They should be expressly illustrative rather than minimum specifications.
- **Underdeveloped examples (Examples 3, 7, 9, 18 and 20).** These examples omit facts needed to apply the test. Each should identify the relevant entity and dataset, describe the concrete re-identification pathway, state access conditions and safeguards, give any relevant thresholds, apply the legal standard step by step and, ideally, show which fact would change the result.
- **Operational benchmarks and unstructured data.** Where possible, the Guidelines should offer practical methods and measurable indicators that engineering teams can build against. For the publication of aggregate data, indicative statistical benchmarks, such as minimum aggregation or cell-size thresholds, would give organisations greater legal certainty, provided they are presented as illustrative reference points rather than mandatory minimum specifications. They should also confirm that the same risk-based approach applies to unstructured data such as free text, transcripts and correspondence, with examples. Metrics such as group-size measures or differential-privacy parameters should be illustrative and assessed in context; no single metric should on its own be conclusive, either as proof of anonymity or as an automatic failure.
- **Terminology (para 40).** We agree that controllers should not describe data as anonymous where individuals remain identifiable. Para 40 however, also bars "de-identified" and "de-

[9] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024.

[10] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216), adopted on 10 April 2014, section 3.

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu

personalised" in that situation. Organisations operating globally use "de-identified" as a term of art defined in other legal regimes, such as US state privacy laws and US health privacy rules, often within a single global privacy notice. Its use should not be treated as misleading where the notice makes clear that the data remains personal data under the GDPR. Para 40 should therefore target only statements suggesting that data falls outside the GDPR when it does not.

5. Conclusion

DOT Europe supports the EDPB's objective of updating its guidance on anonymisation and welcomes the entity-relative approach. To make the Guidelines workable in practice, we invite the EDPB to amend the draft guidance while focusing on three priorities:

1. apply a realistic, foreseeable standard to relevant entities, time and cost, technological developments and reassessment, in line with Recital 26 and CJEU case law;
2. give due weight to all effective safeguards, including contractual measures, and recognise anonymisation within an organisation, for intra-group recipients and by processors;
3. provide legal certainty and practical tools: a clear presumption of anonymity when the criteria are met, positive worked examples, indicative benchmarks, criteria for AI models and synthetic data and guidance on privacy-enhancing technologies.

These changes would encourage organisations to invest in anonymisation, to the benefit of individuals and of data-driven innovation in Europe. DOT Europe and its members remain available to share technical expertise, including through a dedicated workshop, and to continue this dialogue.

Avenue Marnix, 17
1000 Brussels,
BELGIUM

TEL
+32 (0)472 26 83 02

MAIL
info@doteurope.eu

WEBSITE
www.doteurope.eu