DigiData
CONSULTING LTD

DIGIDATA CONSULTATION SUBMISSION

Anonymisation and Identifiability

Submission on the EDPB Guidelines

Guidelines 02/2026 on Anonymisation

Version 1.0 adopted for public consultation on 7 July 2026



Dr Mark R Leiser

DigiData Consulting Ltd

Riga Graduate School of Law

30 October 2026

Submission on the EDPB anonymisation guidelines

Response to Guidelines 02/2026 on Anonymisation
Version 1.0 adopted for public consultation on 7 July 2026

Dr Mark R Leiser | DigiData Consulting Ltd | 30 October 2026

1 A Workable Assessment of Identifiability

The final guidelines should explain how an organisation can reach and substantiate a conclusion about identifiability in a particular processing context. Effective separation may prevent one recipient from identifying individuals while the disclosing organisation retains personal data and responsibility for its own processing. Article 4(1) and recital 26 require an assessment of the means that the controller or another person would reasonably be likely to use to identify an individual.[1]

The draft already recognises that information may be anonymous for one entity and personal for another, and distinguishes contextual assessment from a simplified approach.[2] The final guidance should make the consequences of those distinctions easier to apply. Organisations need to know what evidence supports a conclusion, which processing it covers and what changes require reassessment. Otherwise, they cannot reliably assess the legal consequences of investment in privacy engineering.

The report *Restoring Legal Certainty in EU Data Protection Law* connects the definition of personal data with arrangements for assurance and institutional responsibility.[3] The accompanying anonymisation analysis distinguishes a conclusion about a particular recipient from a claim that a dataset is anonymous in every setting.[4] This submission develops that approach through recommendations for applying existing law. Section 10 addresses proposals that would require legislation.

The recommendations cover five matters: *identifying the relevant entity and processing operation*; *explaining realistic routes to identification, including the ability to distinguish and act upon a person*; *evaluating effective technical, organisational and contractual controls*; *separating general statistical knowledge from disclosures about individuals*; and *recording the evidence on which an organisation relies*. Together, these measures would help supervisors and organisations understand both the reach and the limits of an assessment.

The nine cases below use hypothetical facts to examine how changes in access, purpose, data, or disclosure affect the analysis. They contain no client information or empirical performance claims. The proposals apply the statutory definition of personal data and preserve the controller's duty to demonstrate compliance with applicable GDPR obligations.[5]

2 The Recipient in the Processing Chain

In *EDPS v SRB*, the Court rejected the proposition that pseudonymised information necessarily constitutes personal data for every recipient. The judgment also addresses transfers to third parties capable of identification and the information duties of the collecting controller.[6] An assessment must therefore identify whose processing and which obligation require examination.

The case concerns Regulation (EU) 2018/1725. The Court expressly requires consistent interpretation of its definition of personal data and the corresponding GDPR definition. For the information duty at

[1] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1 (GDPR), recital 26 and art 4(1).
[2] European Data Protection Board (EDPB), Guidelines 02/2026 on Anonymisation (version 1.0, 7 July 2026), paras 6–15 and 47–49.
[3] M R Leiser, Restoring Legal Certainty in EU Data Protection Law: Why the Digital Omnibus Matters for the GDPR and the Digital Acquis (DigiData Consulting Ltd, 18 August 2026), sections 3.2 and 4.4.
[4] M R Leiser, 'Context Is Not a Loophole' (LawBhoy, 10 July 2026).
[5] GDPR, arts 5(2) and 24(1).
[6] Case C-413/23 P *European Data Protection Supervisor v Single Resolution Board* EU:C:2025:645 (*EDPS v SRB*), paras 75–87 and 110–115.

issue, the Court adopted the collecting controller's perspective at the time of collection. It set aside the General Court's judgment and remitted the case.[7] A recipient's later inability to identify an individual cannot retrospectively remove that information duty. The judgment did not determine that the information was anonymous for Deloitte.

An assessment should define its subject before technical testing begins. For example: 'This assessment concerns Institute R's independent analysis of release R3 through access environment M. The hospital's collection, its processor's activities and any subsequent disclosure to a registry require their own assessments.' This opening identifies the operation to which the conclusion applies and prevents an organisation from extending that conclusion to different processing without examining the relevant facts.

The assessment must also address means available through third parties. A recipient may obtain auxiliary information, commission a matching service or disclose records to an organisation that can identify individuals. Those possibilities can affect the classification of the data.[8] The analysis should explain the practical route, including access, relationships, resources and likely further disclosure. Assuming an unspecified actor can access every relevant dataset provides little help in evaluating an actual arrangement.

Paragraph 48 expressly states that the simplified approach does not create an alternative legal standard. Paragraphs 49 and 95–103 explain how further analysis may establish anonymity despite an unsuccessful initial screen.[9] The final text should bring that explanation closer to the screening criteria. Supervisors should evaluate the evidence against the statutory test and explain the significance of the particular result, including whether the analysis has already established a specific and meaningful inference about an identifiable individual.

3 Independent Research and Processing for the Hospital

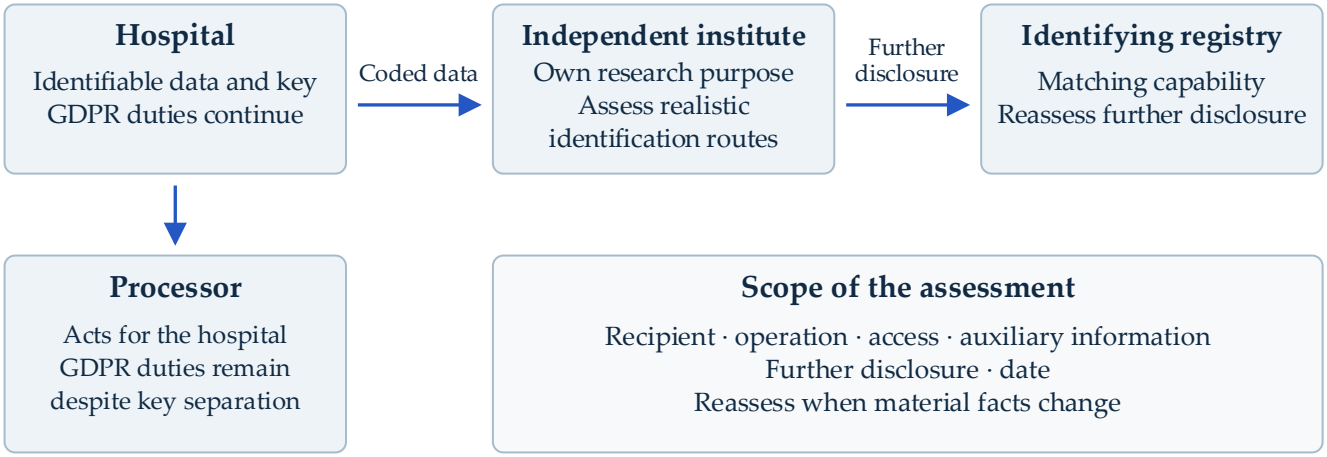


Figure 1 Separate assessments within the same processing chain

Case 1: A hospital and an independent institute. A hospital retains the key that connects coded patient records to names. An institute determines its own research question and methods. The hospital generalises dates and removes free text before disclosure. The institute has no lookup service, and its other holdings offer no realistic way to match the data. These facts require separate examination of the

[7] *EDPS v SRB* (n 6), paras 52, 110–115 and 120–122, and operative part, points 1–2.
[8] *EDPS v SRB* (n 6), paras 77, 79 and 82–87.
[9] EDPB, Anonymisation Guidelines (n 2), paras 48–49 (including n 36) and 95–103.

hospital's and institute's positions. The description 'research partners' establishes neither organisation's legal role.[10]

Before concluding that the data are anonymous for its purposes, the institute must examine the remaining attributes, accessible auxiliary information and foreseeable further disclosure. The hospital continues to process personal data and must establish a lawful basis for the clinical processing and disclosure, together with any applicable Article 9 condition.[11]

Suppose instead that the institute follows the hospital's instructions and returns individual patient results as its processor. The hospital's decision to withhold the key does not, by itself, take that processing outside the GDPR. In another variation, the institute retains independence but gains access to a service that contacts coded patients and returns individual findings. That service may enable the institute to attribute information or act upon patients through the hospital. The revised assessment must account for that capability.

The data may also provide an independent route to identification. A rare diagnosis, exact operation date and small locality may together match details on an identifiable person's public fundraising page. The assessor must evaluate that combination even where the recipient cannot obtain the hospital's key.

The Board should use paired examples to explain the consequences of these changes. Each example should examine actual purposes, instructions, and capabilities so contractual descriptions accurately reflect the processing arrangement.

4 The Evidential Value of Safeguards

A threat model should identify the relevant actor, access route, auxiliary information, resources and method of identification. Security vulnerabilities matter to the scope inquiry when they create a realistic means of identifying a natural person in the relevant setting. The Court asks which means a controller or another person would reasonably be likely to use to identify the individual. A legal prohibition or practical impossibility, including disproportionate time, cost and labour, can make the risk insignificant in reality.[12]

Case 2: A restricted research environment. A recipient cannot export records, upload external matching tables or communicate results about individual rows. Each authorised researcher uses separate credentials, and the operator logs queries and reviews outputs. These restrictions may substantially reduce the recipient's capacity to identify individuals. The assessment must examine the operation: whether administrators can bypass controls, whether researchers share credentials, and whether repeated outputs permit the linkage the restrictions seek to prevent.

Case 3: An agreement against reidentification. A recipient promises not to reidentify anyone but can readily purchase a table connecting retained email hashes to names. The available table remains relevant to the assessment. A different arrangement uses a secret key that the recipient cannot access, restricts inputs and joins, monitors use and imposes enforceable sanctions. The assessor must examine the combined effect of those measures and any remaining matching route.[13]

The guidance should distinguish an assertion of benign intentions from evidence about access, incentives, enforceability and resources. A declaration that an organisation has no intention of identifying individuals establishes little about its capabilities. The cost of identification, the likelihood of detection and credible sanctions may affect whether someone would reasonably be likely to use a particular route. The conclusion should explain the weight that each circumstance carries.

---

[10] GDPR, arts 4(7)–(10), 28(1), 28(3)(a) and 28(10).

[11] GDPR, arts 4(1)–(2), 5, 6 and 9(1)–(2).

[12] *EDPS v SRB* (n 6), para 82.

[13] EDPB, Anonymisation Guidelines (n 2), paras 28–35 and 88–93, especially paras 31, 33–34 and 90–91.

Unlawful access also requires factual analysis. Previous compromises, exploitable systems or incentives for insider disclosure may make a particular attack relevant. The assessor should record the evidence for including or excluding each material route and identify developments that could change the assessment. General references to cybercrime or future computing power need a connection to the data and access arrangements under review.

5 Unique records and routes to identification

Technical diagnostics help organisations apply Article 4(1) when assessors explain their legal significance. A unique record, a possible join and a predictive inference raise different questions. Paragraphs 52–53 and 95–103 already explain that a failed criterion may require further analysis. The final text should make the distinction between isolating a record and identifying a person explicit wherever practitioners encounter the criteria.[14]

Case 4: A survey without an identifying link. A large survey collects answers without identifying attributes, contact details or mapping information. One respondent gives a unique combination of answers, but the analyst has no reasonable means of connecting that combination to a person or acting upon the respondent individually. The assessment must explain what that uniqueness permits in practice. If the respondent publishes the same distinctive answers in an identifiable public post, the assessor must evaluate the resulting matching route.

Case 5: An advertising token. A supplier recognises a user across encounters, combines behavioural information and selects an advertisement for that user. The supplier's capacity to distinguish and address the person remains relevant even without a name. *IAB Europe* also confirms the importance of information that other participants can reasonably make available.[15] An organisation that receives protected campaign totals and cannot distinguish or address individual users presents a different set of facts. The guidance should make those differences explicit.

Assessors should also examine how device identifiers connect to natural persons. A shared terminal, household identifier and individual account can support different conclusions. Evidence about actual use should inform that analysis; an identifier's initial attachment to a device does not resolve the question.

Table 1 Connecting technical diagnostics to the legal test

Diagnostic	Legal question	Evidence to record
Unique record	Can the recipient distinguish or act upon a natural person through this record?	Attribution route and practical use
Possible linkage	Can the recipient obtain and use the matching information?	Access, matching quality and external services
Inference	Does the output reveal information about an individual, and how does it connect to source records?	Link to a person, dependence on source data and reliability

[14] EDPB, Anonymisation Guidelines (n 2), paras 52–53 and 95–103. Case 4 develops the survey in example 24 (para 99).

[15] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* EU:C:2024:214, paras 44–51, especially 48–50; EDPB, Anonymisation Guidelines (n 2), para 25 and example 6.

6 Controlled Access and Publication

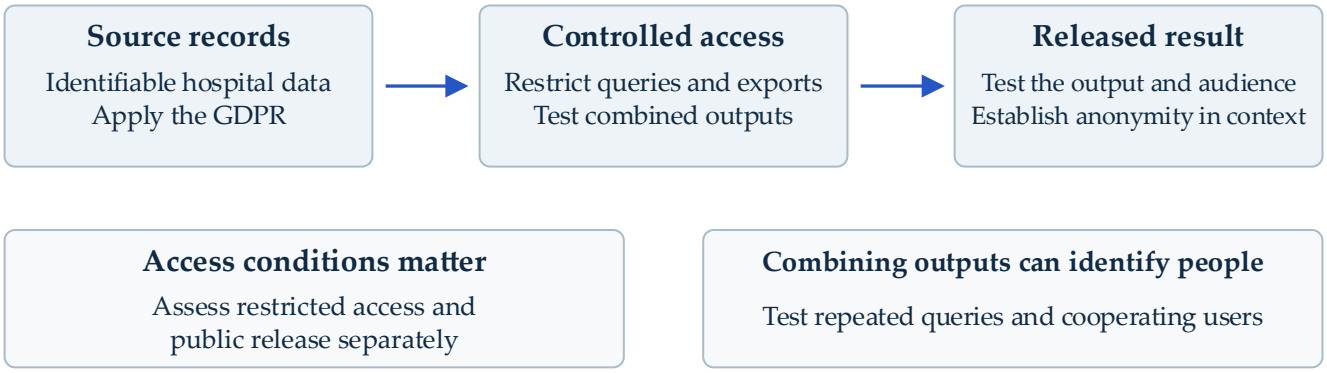


Figure 2 Assess the source records, access route and each released output.

Case 6: A query service. A hospital retains identifiable records. Researchers submit approved statistical queries and receive aggregates after disclosure review. The hospital's processing of the source records remains subject to the GDPR even where a particular output contains no personal data. The assessment should separately address researchers' access, the query service's operation, and the information disclosed through its outputs.[16]

For example, a user obtains the total salary of six staff members and then the total for five known members of that group. Subtraction reveals the sixth person's salary. Repeated queries about overlapping research cohorts can create an equivalent disclosure. Query limits, minimum group sizes and output review must address combinations of results, including combinations that collaborating users can assemble.

Case 7: Publication of search records. Removing account names can leave rare queries, timestamps, and search sequences. A quoted phrase may lead to an identifiable public post. Repeated searches concerning a location or workplace may reveal a particular individual. Public release expands the range of recipients and auxiliary information relevant to the assessment. *OC v Commission* illustrates how contextual details and external information can identify someone whose name does not appear in the initial publication.[17]

A conclusion concerning one accredited institute cannot establish anonymity for unrestricted publication. A release assessment should examine foreseeable recipients, accessible background information, retained detail and the cumulative effect of disclosures. The controller should explain foreseeable uses and circulation on the available evidence, with proportionate provision for review as circumstances change.

Where anonymisation would remove information essential to legitimate research, the organisation should consider whether it can conduct that research as personal-data processing under an appropriate legal basis and safeguards. The guidance should explain the consequences of modifying the data, restricting access and retaining GDPR protection, so that organisations can choose a lawful arrangement suited to the proposed research.

[16] GDPR, recital 26 and arts 4(1)–(2), 5, 6, 9 and 89(1); EDPB, Anonymisation Guidelines (n 2), paras 76–77 and example 16, on combining salary aggregates.
[17] Case C-479/22 P *OC v European Commission* EU:C:2024:215, paras 54–63, especially 59–63. The search-record scenario applies this reasoning by analogy.

7 General Statistical Knowledge and Disclosures about Individuals

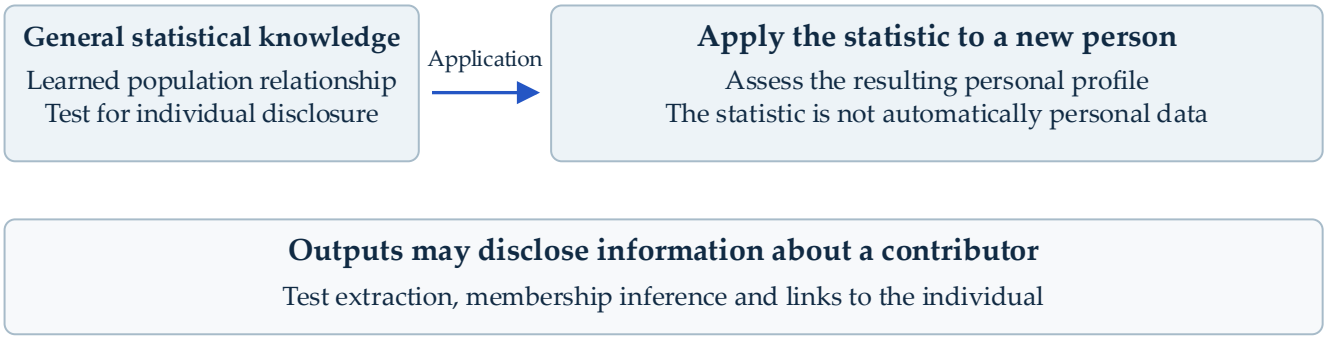


Figure 3 Distinguish general statistical knowledge from disclosures about contributors.

Case 8: A statistic used in lending. A population statistic helps a lender assess a new applicant who did not contribute to the source dataset. The resulting individual profile constitutes personal data. That application alone does not establish that the general statistic contains personal data or that the source records identify their contributors. Paragraphs 69–71 and Example 14 already recognise this distinction.[18] The final guidance should preserve it while explaining how assessors can identify inferences that depend on information about particular contributors.

In a variation, a model reveals that an identifiable person belonged to a small treatment group. Membership may itself disclose a diagnosis. An output can therefore reveal personal information even when it omits a name, provided the recipient can reliably connect the output to the person. The assessment must examine the inference, its relationship to the source records and the recipient's auxiliary information.

Case 9: Synthetic patient records. Generated records resemble real patients but contain invented names. The assessor should test whether rare combinations reproduce source records, whether membership or extraction attacks disclose information about individuals and whether accessible information permits linkage. A supplier's description of data as 'synthetic' does not answer those questions. Aggregates and model parameters require equivalent attention to their content and the recipient's capabilities.[19]

The guidance must also distinguish anonymity from the classification of personal data under Article 9. An uncertain inference about a named person can still constitute personal data. A processing operation may reveal health information without establishing the underlying condition with certainty. In *Lindenapotheke*, the Court accepted the relevance of probabilistic conclusions about health in the circumstances.[20] A technical test of inference must therefore avoid imposing certainty or an intention to infer health information as additional conditions under Article 9.

Assessors should identify the information disclosed about an individual, the means of connecting that information to the person and the significance of its dependence on the source records. When an organisation applies general knowledge to a new individual, the resulting processing requires its own analysis. Paired examples should show how those principles apply to models and synthetic data under different conditions of access and disclosure.

[18] EDPB, Anonymisation Guidelines (n 2), paras 67–71 and example 14; see also paras 72–82.
[19] Leiser, Restoring Legal Certainty (n 3), section 4.4, 31–32.
[20] Case C-21/23 *Lindenapotheke* EU:C:2024:846, paras 83–94, especially 90–91.

8 A Reusable Record of the Assessment

Restoring Legal Certainty proposes an assurance process that ties a claim about anonymity to a particular entity, technical arrangement and range of permitted disclosures.[21] The related analysis of privacy-enhancing technologies argues that organisations need evidence they can examine and, where appropriate, use in subsequent assessments.[22] Reuse should reduce unnecessary duplication while preserving scrutiny of each recipient's circumstances.

The Board should publish a minimum assessment record covering the tested facts, conclusions and limitations. The specimen below concerns the hospital and independent institute. Its illustrative entries do not establish anonymity without evidence that the controls work and that retained attributes offer no realistic identification route.

Table 2 Minimum record for an anonymisation assessment

Field	Illustrative Entry	Response to a Material Change
Recipient and role	Institute R independently conducts study S	Reassess if the institute begins acting on the hospital's behalf.
Release and access	Version R3 within controlled environment M	Assess each new export separately.
Identification routes	Examine key access, rare attributes, public matching and recontact	Reassess access to any new lookup service.
Controls and testing	Separate secrets; restrict joins; review query logs and disclosures	Suspend reliance where a material control no longer works.
Further disclosure	Limit access to the named institute under specified restrictions	Assess any proposed disclosure to an identifying registry.
Accountability	Record reviewer, date, limitations and review triggers	Explain the grounds for each revised conclusion.

The effort needed to support a conclusion should reflect the complexity of the processing and identification routes. A routine aggregate may justify a short assessment; a dataset with many attributes or a downloadable model may require specialist testing. The definition of personal data remains the same. Guidance should explain which evidential gaps prevent a conclusion and which permit a conclusion subject to clearly stated limits. Controllers retain the duty to demonstrate applicable compliance.[23]

A change register should distinguish defects in the original assessment from later developments that alter an initially sound conclusion. Supervisors should examine the evidence and foreseeable means of identification at the relevant time. Specified review triggers and proportionate periodic reassessment can help organisations maintain justified conclusions.

Guidance can explain the evidential value of a documented assessment and encourage consistent supervisory treatment. It cannot amend the statutory definition, relieve a controller of responsibility or displace judicial remedies.[24] A binding statutory presumption requires legislative provision.[25]

[21] Leiser, Restoring Legal Certainty (n 3), sections 3.2 and 8.2–8.3.
[22] M R Leiser, 'Europe Will Not Build a PET Market on Legal Ambiguity' (LawBhoy, 18 August 2026), under 'What PETs need to thrive in a European marketplace'.
[23] GDPR, arts 5(2), 24(1) and 25(1)–(2).
[24] GDPR, arts 24(3), 42(4), 70(1)(e), 78 and 79.
[25] Leiser, Restoring Legal Certainty (n 3), sections 8.2–8.3.

9 Recommended Additions to the Guidelines

The following additions would connect the technical framework more clearly to the statutory test. They build on distinctions that the draft already recognises and would make its assessment method easier to use.

Perspective and operation. Add to section 2.2: 'Identify the relevant entity, processing operation, access arrangements and legal obligation before determining the appropriate perspective. Assess the collecting controller's obligations separately, the position of a processor and any subsequent disclosure to a third party capable of identification. State precisely which recipient and operation the conclusion concerns.' This wording reflects the importance of both recipient capability and the timing of the controller's information duty.[26]

Access through third parties. Clarify paragraphs 21 and 28–35: 'Identify material routes through which an entity may obtain means of identification or disclose data to a party capable of identification. Explain the evidence concerning access, resources, relationships and likely use. Evaluate contractual restrictions alongside the practical means of obtaining or disclosing the information.'

Effective safeguards. Clarify paragraph 34 alongside paragraphs 90–91: 'Evaluate technical, organisational and contractual measures together. Examine access, enforceability, oversight, incentives and opportunities for circumvention. Explain how the measures affect the means of identification reasonably available in the circumstances and identify material residual routes.' The assessment should show what the controls achieve in practice.[27]

Screening and further assessment. Add beside paragraph 52, with cross-references to paragraphs 48–49 and 95–103: 'Explain the legal significance of each screening result. Where a test isolates a unique record, assess whether the recipient can use that record to distinguish or act upon a natural person. Complete any necessary contextual analysis before determining whether the data meet the statutory definition.'[28]

Inference and mixed datasets. Clarify paragraph 36 and paragraphs 66–82: 'Distinguish disclosures about people represented in the source data from the application of general knowledge to another person. Do not describe a dataset containing identifiable records as anonymous as a whole. An organisation that separates and retests a subset may reach a different conclusion for that subset where the evidence supports it.'[29]

Evidence and review. Add an annex containing the minimum assessment record, paired examples and a change register. Explain the recipients and operations to which a conclusion applies, the evidence that supports it and the circumstances that require reassessment. When the Board publishes new attack models, it should explain their relevance to existing assessments and the conditions under which organisations should revisit their conclusions.

[26] *EDPS v SRB* (n 6), paras 75–87 and 110–115; GDPR, arts 4(8), 4(10) and 28; EDPB, Anonymisation Guidelines (n 2), paras 11–15.
[27] EDPB, Anonymisation Guidelines (n 2), paras 34 and 90–91.
[28] EDPB, Anonymisation Guidelines (n 2), paras 48–49, 52–53 and 95–103.
[29] EDPB, Anonymisation Guidelines (n 2), para 36 and paras 66–82.

10 Supervisory responsibility and legislative reform

The final guidelines should explain how supervisors will assess supported conclusions consistently. Cumulative assumptions about hypothetical actors, access and future capabilities must not displace the contextual inquiry. The practical difficulty becomes particularly acute where other legislation requires data access. The cited analyses of the proposed Article 6(11) DMA search-data remedy examine the role and limits of recipient controls and later enforcement.[30,31]

The Board should publish reasoned responses to material objections, maintain examples showing the effect of changed facts, and provide a proportionate evidence template. Where several methods meet the applicable legal requirements but preserve different levels of utility, the Board should explain the reasons for its recommendation. Where evidence remains uncertain, it should specify the uncertainty and identify research that would help resolve it.

The guidance should also explain the boundaries between legal regimes. Producing an anonymous output does not remove the GDPR obligations that govern the processing of its personal-data sources. Similarly, an output's origin does not, by itself, determine whether each recipient processes personal data. Other rules may address misuse, discrimination or contractual misconduct.[32] Article 5(3) of the ePrivacy Directive separately regulates storage of information in terminal equipment and access to information already stored there, including non-personal information, subject to its conditions and exceptions.[33]

The Council agreed its negotiating mandate on 21 October 2026. The mandate proposes a new Article 25a on pseudonymisation, including recipient-specific assessment and identifying onward disclosures; it does not amend current law.[34] Legislators should define when a recipient can rely on anonymity, preserve responsibility for reasonably foreseeable identifying disclosures, and determine the legal effect of approved assurance arrangements. Meanwhile, the Board should help organisations apply existing law.

The Innovation Mandate proposes duties to examine evidence, consider proportionate alternatives and give public reasons when institutions choose among lawful options.[35] Those proposals preserve fundamental-rights requirements. Legislative reform could establish binding institutional duties, while the Board can already explain its evidence, clarify its methodology and recognise the practical effects of effective safeguards.

The requested guidance would allow an organisation to reach a supported conclusion for a named recipient, a defined operation and specified access and disclosure arrangements. It would also identify the changes that require review. That combination would make compliance more predictable and give practical effect to the contextual assessment of identifiability.

---

[30] M R Leiser, 'Anonymisation, Two Ways' (LawBhoy, 13 July 2026).

[31] M R Leiser, 'Anonymous Enough to Share, Personal Enough to Police?' (LawBhoy, 18 June 2026).

[32] GDPR, recital 26 and arts 2(1), 4(1)–(2) and 70(1)(e); *EDPS v SRB* (n 6), paras 75–87.

[33] Directive 2002/58/EC [2002] OJ L201/37, art 5(3), as amended by Directive 2009/136/EC [2009] OJ L337/11; Case C-673/17 *Planet49* EU:C:2019:801, paras 68–71.

[34] Council of the European Union, Digital Omnibus: Mandate for negotiations with the European Parliament, ST 14756/26 (22 October 2026), cover note and annex, art 3(10), proposed GDPR art 25a, 140–141.

[35] M R Leiser, The Innovation Mandate: Making Europe's Digital Supervisory State Accountable for Rights, Growth and Scale (DigiData Consulting Ltd, July 2026), sections 5.1–5.3 and 9.1.

DigiData
CONSULTING LTD

About this submission

Authorship and professional context

Dr Mark R Leiser is a legal academic at the Riga Graduate School of Law and director of DigiData Consulting Ltd. He undertakes research and consultancy for public bodies, private companies and civil society organisations. This submission presents his legal analysis and recommendations. References to other organisations do not imply their endorsement.

Scope and examples

This submission responds to Guidelines 02/2026 on Anonymisation and reflects the cited legal and policy materials as at 30 October 2026. It distinguishes interpretation of existing law from proposals for legislative reform.

The nine worked cases use hypothetical facts. They do not describe client matters or report empirical testing. Any practical assessment must address the actual data, participants, safeguards and means of identification.

Copyright and citation

© 2026 Dr Mark R Leiser. All rights reserved. Third-party material remains subject to the rights of its respective owners.

Suggested citation: Mark R Leiser, *Submission on the EDPB Anonymisation Guidelines* (DigiData Consulting Ltd, 30 October 2026).

Please direct enquiries and requests to reproduce original material to DigiData Consulting Ltd.

CONTACT

DigiData Consulting Ltd

enquiries@digidata.uk

digidata.uk

Registered in Scotland · SC734919

