Contribution to the EDPB Public Consultation

on the Guidelines 02/2026 on Anonymisation (v1.0, 07 July 2026)

Observations from the perspective of a Lawyer and Data Protection Officer:
Submitted by: Avv. Francesco Luongo — Cassazionista, Lawyer, Data Protection Officer
Contribution category: DPO / Individual
Country: Italy — www.linkedin.com/in/francesco-luongo
Sector: Professional and technical activities; public-law professional bodies

1. Premise and Position of the Contributor

This contribution is submitted in a personal and professional capacity, drawing on direct experience as the appointed Data Protection Officer of a professional body governed by public law — specifically a non-economic public body within the meaning generally attributed to professional Bar Associations under Italian administrative law — and on parallel experience as a cassation-level lawyer handling litigation, disciplinary matters and consumer protection files.

This opinion is submitted solely in a personal and professional capacity and does not represent the formal position of any public body or client.

The observations below are grounded in concrete operational practice: the drafting and periodic update of a Register of Processing Activities and a Data Protection Impact Assessment for a Bar Association and its affiliated bodies (mediation body and over-indebtedness composition body), the qualification of external processors, and the recurring need to produce anonymised or statistical outputs from registers, disciplinary files and case-management systems that are, by their nature, populated with data subjects belonging to a closed and largely known professional community.

This standpoint is relevant to the present consultation because professional bodies, judicial observatories, mediation and over-indebtedness composition bodies share a structural feature that the draft Guidelines do not yet fully address: the population from which their datasets are drawn is not an open, anonymous crowd, but a closed and largely identifiable professional or procedural community (registered members, parties to proceedings, disciplinary respondents), a scenario materially different from the open-population case studies (surveys, social media, aggregate statistics) that dominate the Guidelines' worked examples.

2. General Assessment

The Board's initiative to update the 2014 Article 29 Working Party framework, incorporating subsequent CJEU case-law (notably EDPS v SRB and Breyer) and offering both a contextual and a simplified approach, is welcomed. The three-criteria framework — No Record Isolation, No Linkage, No Inference — provides a workable, technology-neutral structure that can, in principle, be applied by controllers of very different size and sophistication.

The observations that follow are offered in that constructive spirit. They do not question the soundness of the framework; they aim to ensure that its application remains coherent and genuinely workable for controllers operating within closed, professionally-defined populations and with limited compliance resources — a category that includes small public-law bodies and regulated professionals, alongside the large private controllers for which several worked examples appear to have been primarily designed.

3. Closed, Known-Membership Populations: a Category the Framework Does Not Fully Address

Example 22 (paragraphs 88–94) illustrates the contextual approach through a research institute whose members "had no direct interaction with the patients" and have "no record of which patients were included in the dataset" — the conclusion being that no relevant entity would even know that a given individual's data was included. This scenario does not transpose well to professional bodies. Where a Bar Association, a mediation body or an over-indebtedness composition body produces anonymised statistics from its registers or disciplinary files, the professional counterparts of the data subjects — colleagues on the governing Council, opposing counsel, mediators, judges, the registry secretariat — routinely already know, or can trivially infer, that a specific individual's data is included, because registration and participation in the relevant proceeding are matters of ordinary administrative or procedural record, quite independently of the dataset under assessment.

In such cases the confidential element is not membership in the underlying population (which is already known or knowable through ordinary professional channels), but the specific attribute values attached to that membership (e.g. the nature of a disciplinary sanction, the outcome of a mediation, the quantum of a debt). The Guidelines' No Record Isolation and No Linkage criteria, as currently illustrated, do not squarely address this variant, in which the risk of singling out arises less from establishing that an individual is "in" the dataset and more from attaching a sensitive attribute to an individual whose presence is never in doubt.

Recommendation: the Board should consider adding a worked example addressing closed, known-membership populations (professional registers, disciplinary files, judicial or procedural datasets), clarifying how the No Record Isolation and No Linkage criteria should be applied where membership itself is not the element requiring protection, and how the No Inference criterion interacts with attribute-level confidentiality in that setting.

4. Professional Secrecy and Statutory Confidentiality as a "Means Not Reasonably Likely to Be Used" Factor

Paragraphs 32–34 rightly distinguish a prohibition set out in law, which may render a means not reasonably likely to be used, from a prohibition set out in a contract, which the Guidelines direct assessors to treat with more caution given that contractual measures "can typically be subject to revision, or may even be disregarded entirely by the parties."

This binary treatment does not fully capture the legal position of professional secrecy as it applies to lawyers, mediators and similar regulated professionals under Italian law. Legal professional secrecy is not a matter of private contract: it is a criminal-law duty (Article 622 of the Criminal Code), a deontological duty enforceable through disciplinary sanction up to disbarment (Articles 13 and 28 of the Codice Deontologico Forense, the latter expressly providing, at paragraph 5, for the disciplinary sanction of censure and, where the violation concerns professional secrecy specifically, suspension from professional practice for a period of one to three years), and a procedural privilege recognised in both civil and criminal procedure (Article 249 of the Code of Civil Procedure; Article 200 of the Code of Criminal Procedure). Functionally, it sits much closer to a "prohibition by law" than to an ordinary contractual non-disclosure clause, since it is backed by criminal and disciplinary sanction — the latter quantified and independent of any agreement between the parties — and cannot be waived by contract.

Recommendation: the Guidelines should expressly acknowledge that statutory or deontological secrecy obligations backed by criminal or disciplinary sanction — as distinct from purely contractual confidentiality clauses — may properly be weighed closer to a prohibition by law under paragraph 32, though not as an

automatic or conclusive anonymisation guarantee, and without prejudice to the assessor still verifying, per the rebuttal factors listed at paragraph 33, that the obligation is in fact effectively monitored and enforced in the professional community concerned.

5. Small Public-Law Controllers and the Practical Cost of the Contextual Approach

Paragraphs 47–49 rightly leave controllers the choice between a contextual and a simplified approach, and encourage combining both. In practice, however, non-economic public bodies such as Bar Associations, mediation bodies and over-indebtedness composition bodies typically operate with very limited in-house legal, IT and budgetary resources for compliance. For such controllers the simplified approach is understandably attractive, but its acknowledged risk of over-classifying data as personal (a false negative in anonymisation terms) has a real proportionality cost: it can obstruct legitimate institutional reporting — for example aggregate disciplinary statistics, or mediation and over-indebtedness outcome reports — that transparency obligations applicable to public-law bodies may in fact require.

Recommendation: the Board should consider including, alongside the general guidance at paragraphs 47–49, a simplified worked decision-path calibrated to typical small-controller scenarios (registry extracts, disciplinary or procedural statistics), so that resource-constrained public-law bodies are not systematically pushed towards a more conservative, and potentially less proportionate, application of the simplified approach than the underlying risk would justify.

6. Mixed Datasets in Family, Disciplinary and Judicial Proceedings

Paragraph 36 correctly states that a dataset containing a mix of personal and anonymous data must, in the absence of separate treatment, be handled as containing personal data as a whole, and that anonymisation of a dataset requires the likelihood of re-identification to be insignificant for all included individuals. Case files arising from family-law, disciplinary or judicial proceedings routinely combine data of markedly different sensitivity and different data subjects within the same file — the parties themselves, but also minor children who are not parties, witnesses, and third parties incidentally mentioned (health conditions, addiction, financial distress).

Recommendation: where anonymisation is applied to court-derived or proceeding-derived datasets for research, statistical or institutional-reporting purposes (for instance by a Bar Association or a judicial observatory), the Guidelines should clarify that the "all included individuals" test at paragraph 36 must be applied separately to each category of data subject present in the file, since minors and incidentally-mentioned third parties typically present a materially higher re-identification risk profile than the named parties to the proceeding, owing to the far smaller pool of comparators.

7. Interplay with AI Act Documentation Obligations

Anonymisation is increasingly relevant not only as a stand-alone compliance exercise but also as a gateway enabling the lawful re-use of professional or judicial data for training or fine-tuning AI systems supporting the legal profession. The documentation duties described at paragraph 41 (retention of records demonstrating both the GDPR-compliance and the technical effectiveness of the anonymisation process) may overlap with the data-governance and technical documentation obligations under Regulation (EU) 2024/1689 (the AI Act), in particular for providers of high-risk AI systems or providers of general-purpose AI models where anonymised or supposedly anonymised datasets are used for training, validation, testing or fine-tuning.

Recommendation: the Board should consider a cross-reference clarifying that the documentation produced to satisfy paragraph 41 can, and should, be designed so as to also support the corresponding AI Act data-governance and technical-documentation obligations where they apply, in particular for providers of high-risk AI systems and providers of general-purpose AI models, avoiding duplicative or inconsistent audit trails for organisations — frequently smaller organisations — that must simultaneously answer to both frameworks.

8. Conclusions

The contributor supports the adoption of the updated Guidelines and considers the three-criteria framework a sound and durable basis for assessing anonymisation. The observations above are intended to ensure that the final version remains equally workable for controllers operating within closed, professionally-defined populations and with modest compliance resources, not only for large private undertakings processing open, anonymous crowds of data subjects.

In summary, it is respectfully suggested that the Board consider: (i) adding a worked example addressing closed, known-membership populations such as professional registers and disciplinary or procedural datasets; (ii) clarifying the weight to be given to statutory and deontological professional-secrecy obligations, as distinct from purely contractual confidentiality, when assessing means reasonably likely to be used; (iii) offering a simplified decision-path calibrated to small public-law controllers; (iv) clarifying that the "all included individuals" test under paragraph 36 should be applied separately by category of data subject in mixed judicial or disciplinary files; and (v) cross-referencing the documentation obligations under paragraph 41 with the AI Act data-governance and technical-documentation obligations that may apply, in particular for providers of high-risk AI systems and providers of general-purpose AI models.

The contributor remains available to provide further detail or practical examples on any of the points raised, and thanks the Board for the opportunity to contribute to this consultation.

Yours faithfully,
Avv. Francesco Luongo