Contribution to the EDPB Public Consultation

on the Template for Personal Data Breach Notification (v1.0, 8 June 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

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.

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 management of the Register of Processing Activities (Art. 30 GDPR), the conduct of Data Protection Impact Assessments (Art. 35 GDPR), the maintenance of an internal data breach register (Art. 33(5) GDPR), and the day-to-day handling of relationships with external processors and the organisation's digital infrastructure.

This standpoint is relevant to the consultation because professional bodies, Bar Associations, Mediation bodies (ODM)[1], Over-indebtedness composition bodies (OCC)[2] and public-law professional registers share a common feature that the draft template does not yet fully address: they process data that is frequently covered by professional secrecy, legal privilege, or equivalent statutory confidentiality, and they operate with organisational structures — often lean, sometimes entirely reliant on external processors — that differ materially from those of large private undertakings for which several fields of the template appear to have been primarily designed.

[1] Mediation bodies (Organismi di Mediazione – ODM) are entities registered with the Italian Ministry of Justice and entrusted with the management of civil and commercial mediation procedures under Italian law. In that context, they may process personal data relating to parties, lawyers, mediators and other persons involved in mediation proceedings, including legal, financial and case-related information.

[2] Over-indebtedness composition bodies (Organismi di composizione della crisi da sovraindebitamento – OCC) are bodies registered with the Italian Ministry of Justice and involved in procedures concerning over-indebted debtors under Italian insolvency and debt-restructuring legislation. Their activities may involve the processing of personal data relating to debtors, creditors, professionals and other parties, including legal, financial, patrimonial and case-related information.

2. General Assessment

The Board's initiative to harmonise the format and content of personal data breach notifications across the European Economic Area is broadly welcomed. A common structured template reduces fragmentation among national supervisory authorities, increases predictability for controllers operating in multiple Member States, and — if correctly calibrated — can shorten the time required to produce a compliant notification within the constraints of Article 33 GDPR.

The observations that follow are offered in that constructive spirit. They do not question the merit of the harmonisation exercise; they aim to ensure that the template, once implemented as an IT tool by national authorities, remains proportionate, internally consistent, and genuinely usable by controllers of varying size, nature and organisational complexity — including small public-law bodies and professionals who do not operate dedicated compliance departments.

3. Proportionality and Coherence in the Initial 72-Hour Phase

Article 33 GDPR requires notification without undue delay and, where feasible, within 72 hours of becoming aware of the breach — a standard that explicitly anticipates incomplete information at the time of the initial notification. The template already recognises this through the New/Follow-up Notification distinction (Field 3) and the Complete/Incomplete/Withdraw sub-type (Field 4). The structural concern is not the absence of this mechanism but that it may prove too rigid in certain operational contexts.

Numerous fields restrict residual or uncertain values — "To be determined", "Not yet known", "Number cannot be determined" — to incomplete notifications only (e.g. Fields 44, 56, 57, 61, 65, 67, 70, 72, 89, 97). This design assumes that informational uncertainty is always transitional and will be resolved through a subsequent, fully complete follow-up notification. Operational experience — including with external processors who are not always immediately cooperative, or with infrastructure shared across multiple controllers — shows that some data points (for instance, the exact number of data subjects affected by a breach occurring on a system operated by a third party) may remain genuinely unascertainable even after a reasonable follow-up period, without this amounting to incompleteness of the notification process in the sense intended by Article 33.

Recommendation: the template should distinguish between a temporary "to be determined" value — which triggers an expectation of follow-up — and a stable "not reasonably ascertainable" value, which closes that specific data point without requiring the notification to remain indefinitely classified as incomplete.

A related point concerns Field 49 ("Reasons for late notification"), whose visibility condition is tied to a comparison between "date of awareness + 72h" and "current time". As drafted, this logic risks anchoring the 72-hour assessment to the moment the form is being rendered or completed, rather than to the moment of actual submission to the authority. Given that the production of a notification within a public-law body may involve internal validation, authorisation, or signature steps that a private undertaking would not necessarily require, the calculation should be expressly anchored to the submission timestamp.

4. The Role of the Data Protection Officer in the Notification Process

The template provides for the reporting person to act in the capacity of DPO, legal representative, or other authorised representative (Field 23), and includes a distinct "Accuracy & Responsibility" field (Field 26), whose associated business logic is currently limited to the circular instruction "optional field, implement only if required". The template does not, on its face, assign to the DPO any personal responsibility for the substantive accuracy of the information reported.

Nonetheless, the absence of an express clarification on this point creates a foreseeable risk: when national supervisory authorities implement Field 26 as an IT tool, without further guidance the DPO acting as reporting person could, in practice, come to be treated as personally certifying the accuracy of technical information that originates from — and remains within the responsibility of — the controller. Such an outcome would be inconsistent with Articles 38(3) and 39(1) GDPR and with the consistent position of the former Article 29 Working Party (and subsequently the Board) that the DPO advises and monitors compliance but does not bear personal liability for the controller's compliance failures.

Recommendation: the tooltip accompanying Field 26 should expressly state that, where the reporting person acts in the capacity of DPO, the accuracy declaration concerns the faithful transmission of information provided by the controller, and does not transfer to the DPO any substantive responsibility for the underlying facts of the breach or for the adequacy of the controller's technical and organisational measures.

5. Professional Secrecy and Legal Privilege as a Category of Affected Data

This is, in the contributor's assessment, the most significant substantive gap identified in the draft template. Field 70 ("Type of breached data") lists twenty detailed categories — including biometric, health, genetic, criminal, and financial data — but contains no category for data covered by professional secrecy or legal privilege: client files, privileged correspondence between lawyer and client, documents relating to ongoing judicial or disciplinary proceedings, mediation records, or files of over-indebtedness composition procedures.

The omission is internally inconsistent with the template itself. Field 85 ("Nature of the potential impact for the data subject") already includes, as option i), "Loss of confidentiality of personal data protected by professional secrecy" — meaning the template recognises professional secrecy as a possible consequence of a breach, but does not recognise it as a category of data at the point where the nature of the affected data is first classified. A controller completing the notification is therefore required to describe the impact of a professional-secrecy breach without ever having been invited, earlier in the form, to flag that the data at stake belonged to that category in the first place.

Recommendation: introduce in Field 70 an additional category — for instance "Data covered by professional secrecy, legal privilege or equivalent statutory confidentiality (e.g. lawyer-client files, mediation records, disciplinary or judicial proceeding documents)" — so that the classification of affected data and the assessment of potential impact in Field 85 are built on a coherent informational basis throughout the notification.

6. Categories of Data Subjects in the Legal and Public-Law Sector

Field 65 lists ten categories of data subjects (customers, employees, military or law enforcement staff, minors, patients, students, subscribers, users, vulnerable individuals) plus an open residual option j) for additional categories to be specified in free text. The existing residual option already allows controllers in the legal and public-law sector to describe their specific data subjects, so the present observation is offered as a refinement rather than as the closing of a structural gap.

For controllers such as Bar Associations, mediation bodies, over-indebtedness composition bodies, and public or quasi-public legal service providers, recurring categories include: members of professional registers, applicants for legal aid, parties to proceedings, parties to mediation, debtors and creditors in composition procedures, and whistleblowers or reporting persons under applicable whistleblowing legislation.

Recommendation: add these categories as predefined options under Field 65, both to spare such controllers the systematic use of free-text description and to allow the Board to produce more granular sector-specific statistics from the aggregated notification data, which is one of the stated purposes of the harmonised template.

7. Cross-Border Processing Fields: Allowing Progressive Qualification

The architecture of Section 6.2 (Fields 112–118) is technically sound, but two aspects merit refinement from an operational standpoint.

First, Field 113 already provides an "Unknown" option for the existence of cross-border processing, but this value is not coupled with any structured expectation of a follow-up determination. "Unknown" reads as a terminal answer, whereas the determination of the lead supervisory authority and of the Member States concerned is often a matter that can and should be clarified shortly after the initial notification, particularly in incidents involving cloud service providers or processors established in multiple jurisdictions. A semantic distinction between "Unknown" (no expectation of resolution) and "Under assessment" (resolution expected, to be confirmed in a follow-up notification) would better reflect this reality and avoid premature, potentially inaccurate qualifications being locked into the initial notification.

Second, Fields 117 and 122 require an approximate number of affected data subjects for each selected EEA country. For controllers whose user base is genuinely national but only exceptionally structured by Member State of residence — as opposed to digital platforms with granular telemetry — this level of disaggregation can compel the production of estimates unsupported by any real underlying data, which is of limited value to the lead supervisory authority and may in fact be misleading.

Recommendation: (i) replace or supplement "Unknown" with an "Under assessment" value wherever the cross-border qualification is pending rather than definitively unknowable, with a corresponding expectation of follow-up; (ii) allow an aggregated "EEA (excluding home Member State)" estimate as an alternative to full country-by-country disaggregation, reserving the latter for controllers that genuinely possess that level of granularity.

8. Categorisation of Public-Law Controllers (Field 14/15)

A further structural point, separate from the contributor's own institutional position but identified through the same line-by-line analysis of the template, concerns the binary "Sector"

field (Field 14: Private/Public) and its consequence on Field 15 ("Type of organisation": Freelance or Microenterprise / SME / Large Enterprise / Others), which is visible "only if private".

Public-law bodies are not a homogeneous category for the purposes that Field 15 is designed to capture — namely, organisational scale and the proportionality of expected security measures. A non-economic public body such as a professional Bar Association, typically organised with limited staff and budget, and a public economic body operating in sectors such as energy, transport or public health under company-like governance, present materially different risk profiles and resourcing capacities, yet both are currently collapsed into the single undifferentiated value "Public" with no further qualification available.

Recommendation: make Field 15 (or an equivalent dimensional classification) available regardless of the value selected in Field 14, so that the organisational scale of any controller — public or private — can be captured consistently and used proportionately in the assessment of the adequacy of measures adopted.

9. Communications to data Subjects

The template should also support controllers in ensuring coherence between the notification to the supervisory authority under Article 33 GDPR and any communication to data subjects under Article 34 GDPR. Where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the communication to data subjects must be understandable, practical and capable of enabling individuals to take protective action.

Recommendation: the fields concerning communication to data subjects should encourage controllers to describe, in clear and non-technical language, not only the nature of the breach and the measures taken by the controller, but also the concrete steps that affected individuals may reasonably take to protect themselves, where such steps are applicable.

10. Conclusions

The contributor supports the adoption of a harmonised template for personal data breach notification and considers the initiative a meaningful step towards reducing fragmentation across the European Economic Area. The observations above are intended to ensure that the final version of the template remains genuinely operative and risk-based, and that it is workable not only by large, highly structured organisations, but also by small public-law bodies, professional associations, and professionals who do not operate dedicated compliance functions.

In summary, it is respectfully suggested that the Board consider: (i) distinguishing temporary informational gaps from permanently unascertainable data points; (ii) clarifying that the DPO, when acting as reporting person, does not thereby assume personal responsibility for the substantive accuracy of the controller's information; (iii) introducing professional secrecy and legal privilege as an explicit category of affected data, consistently with the impact already recognised in Field 85; (iv) enriching the categories of data subjects relevant to the legal and public-law sector; (v) allowing progressive, rather than binary, qualification of cross-border

processing; (vi) enabling dimensional classification of public-law controllers on the same basis as private undertakings.

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