A Position Paper on the EDPB Template for Personal Data Breach Notification under Article 33 GDPR

Public consultation response - EDPB "Template for the notification of personal data breaches under Article 33 GDPR", version 1.0, adopted 8 June 2026 (121st plenary), published 10 June 2026. Consultation open until **5 August 2026**.

Authors: Nicola Franchetto (Attorney-at-law admitted in Italy) and Martim Taborda Barata (Attorney-at-law admitted in Portugal)

Licence: This position paper and the accompanying technical artefacts (JSON Schema, field catalogue, OpenAPI specification) are released under **Creative Commons Attribution 4.0 International (CC BY 4.0)**. They are intended for **free adoption by Data Protection Authorities, the EDPB and EDPS** (though this Paper is not specifically adapted to provisions of Reg. 2018/1725) without restriction. See Section VI.

Date: July 2026. **Status**: draft for internal validation before submission.

[A Position Paper on the EDPB Template for Personal Data Breach Notification under Article 33 GDPR]
- [Executive summary]
- [Part I - General comments]
  - [I.1. Overall assessment (positive)]
  - [I.2. Proportionality toward SMEs (a stated target audience)]
  - [I.3. A guided pre-assessment stage (ICO model)]
  - [I.4. Severity assessment: anchor the methodology field to ENISA (with a stated threshold)]
  - [I.5. Misalignment of severity scales]
  - [I.6. Channel versus format]
- [Part II - Comparison with international best practice and derived proposals]
  - [II.1 - Italy (Garante per la Protezioni dei Dati Personali): transition from a national form to the common template]
  - [II.2 - UK (ICO): the guided self-assessment]
  - [II.3 - Australia (OAIC) and Singapore (PDPC): individual-facing/confidential separation and clear triggers]
  - [II.4 - USA (California AG, FTC HBNR): transparency and sectoral models]
  - [II.5 - Canada (OPC/PIPEDA): record-keeping of all breaches]
  - [II.6 - International standards: aligning with ISO/IEC 27035]
  - [II.7 - Comparative value summary]

Part III - EDPB Template section-by-section comments
Section 1 - Notification type
Section 2 - Controller and notifier
Section 3 - Initial breach information
Section 4 - Further information (the assessment core)
Section 5 - Communication to data subjects
Section 6 - Other aspects (cross-border, other authorities)
Section 7 - Attachments
Part IV - Machine-readable standardisation and an optional M2M channel
IV.1 - The proposal
IV.2 - Policy arguments
IV.3 - Voluntariness and proportionality
IV.4 - Security of the channel (Article 32 by design)
IV.5 - Forward-compatibility with the Digital Omnibus single reporting entry point
IV.6 - Multilingual consistency of the controlled vocabulary
IV.7 - Reference implementation (annex)
Part V - Summary of proposals
Part VI - Licence and free adoption

Executive summary

The "Template for personal data breach notification" published by the European Data Protection Board on 10 June 2026 (version 1.0, open for public consultation until 5 August 2026, and therefore a draft not a settled text) ("**EDPB Template**") is a substantial step toward harmonising the notification procedures for personal data breaches under Article 33 of Regulation (EU) 2016/679 ("**GDPR**") across the European Union. This paper endorses its core strengths - its common 23-category personal data breach nature taxonomy, embedded conditional logic and developed sections on breaches involving cross-border processing - and proposes a set of incremental, additive improvements drawn from a comparative analysis of mature notification procedures (such as those made available by the competent data protection authorities of the United Kingdom, Australia, Singapore, United States of America and Canada) and 'and adjacent international methodologies and standards (the ENISA severity assessment methodology; ISO/IEC 27035 on information security incident management).

This Position Paper develops 4 ideas in particular:

1. the addition of a prior **guided pre-assessment** stage, modelled on the approach taken by the UK Information Commissioner's Office, to triage and pre-fills the EDPB Template in specific notification procedures;

2. explicitly anchoring Sections 4.1 & 4.2 of the EDPB Template (on the assessment of likely consequences, potential adverse effects on data subjects, and risks to the rights and freedoms of natural persons which a personal data breach may present) to the methodology for the assessment of severity of personal data breaches published by the European Union Agency for Cybersecurity ("**ENISA"**) on 20 December 2013, with a stated minimum severity threshold for a personal data breach to be subject to GDPR notification obligations;

3. combining the EDPB Template's notification procedure with a **personal data breach record-keeping** framework modelled on the Canadian PIPEDA regime, giving operational shape to the Article 33(5) GDPR documentation duty; and

4. aligning the EDPB Template with **ISO/IEC 27035**'s terminology and incident lifecycle framework.

5. treating multi-regime interoperability as a design goal, by adapting the EDPB Template to also address the NIS2 and DORA incident-notification requirements, so that one structured notification can help satisfy multiple obligations.

This Paper also proposes the creation of a standardised machine-readable schema for personal data breach notification, along with the development of alternative machine-to-machine notification channels, illustrating these proposals through an included reference open-source implementation (JSON Schema, controlled terminology, GDPR field-to-article map) released under CC BY 4.0 and made freely available to the EDPB, European Data Protection Supervisor (though the Paper and this mentioned implementation have not been specifically adapted to the provisions of Regulation [EU] 2018/1725) and EU Member State GDPR supervisory authorities are free to adopt.

Part I - General comments

I.1. Overall assessment (positive)

The template is a meaningful advance toward a harmonised Article 33 GDPR breach notification format. Three features deserve explicit praise:

- A **common taxonomy of 23 incident nature types** plus a 4-quadrant cause classification (internal/external × malicious/non-malicious): this represents an unprecedented shared European vocabulary that may reduce the heterogeneity of notifications and enable comparable aggregate statistics across DPAs;
- **Embedded conditional logic**: in particular, the delay-justification field auto-triggered beyond 72 hours, linked to Article 33(1) GDPR (Field 49 EDPB Template) and the Article 34(3) exemptions coded as structured options (Field 100 EDPB Template): procedural compliance is guided by the form itself; and

- **Developed sections on breaches with cross-border implications** (requiring, e.g., identification of the lead supervisory authority under Article 56 GDPR - Field 114 - , the controller's countries of establishment - Field 115 - , the number of affected data subjects per country - Fields 117 & 122 - and the EEA GDPR supervisory authorities notified or to be notified - Fields 118 & 123): it answers a real need of multinationals, who, today, are required to face different notification forms, in different languages, with different taxonomies, during the most critical 72 hours after becoming aware of a relevant breach.

I.2. Proportionality toward SMEs (a stated target audience)

The Template expressly contemplates SME notifiers (field 15, Section 1.1). However, the EDPB Template's form of **126 rows (100 input fields)** across 7 sections, even with its conditional logic, can be daunting for small undertakings without a data protection officer/counsel or structured data protection team, especially considering the already pressing 72-hour deadline for personal data breach notification.

Proposal: Introduce a **simplified "SME Track"** to be used by controllers who are natural persons or legal persons that meet the requirements of Commission Recommendation 2003/361/EC. This track would, in a first instance, expose only the minimum subset of fields required by Article 33(3) GDPR (nature - Field 55; categories and approximate number of affected data subjects and records - Fields 65, 68, 70 & 73; likely consequences - Fields 79, 81 and/or 83, as applicable; measures taken or proposed to address the breach and mitigate its effects - Section 4.3), deferring the detail fields to a follow-up stage. The conditional logic already present makes this feasible without a second form. This proposal is complementary to the guided pre-assessment proposed in the following Section of this Paper and the machine-readable channel proposed in Part IV of this Paper: SMEs would use this Track, whereas structured organisations would use automation.

I.3. A guided pre-assessment stage (ICO model)

The UK Information Commissioner's Office ("**ICO**") makes a **self-assessment tool** available to organisations, set up as a guided decision tree (is it a breach? → risk? → report to the ICO? → inform data subjects? → document), which can help those organisations decide whether a breach must be reported to the ICO at all. It is accompanied by published examples to illustrate the difference between above- and below-threshold breaches (with only the former being subject to mandatory notification) (ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/).

Whether or not a breach should be notified under Article 33 GDPR is, in itself, a legal judgment, to be made under time pressure. Providing a guided pre-assessment to assist with this judgment, sitting **upstream of the EDPB Template**, could:

1. help organisations triage potential notifications based on whether a notification obligation arises under Article 33 GDPR and whether the Article 34 communication duty arises (high risk), potentially lowering the number of defensive/precautionary breach notifications made (which burden supervisory authorities without legal need and dilute the signals sent by more serious breach notifications); and

2. be leveraged to **pre-fill** the EDPB Template with input already gathered during the pre-assessment (e.g., whether the incident may amount to a confidentiality, integrity and/or availability breach; the cause of the breach; which categories of personal data were affected; circumstances increasing or lowering data subject identifiability in the affected data), so that the organisation does not need to enter the same information twice.

Proposal: Develop a **guided pre-assessment** flow - a short decision flow meant to establish whether GDPR notification duties for a given incident and which carries input received forward into the EDPB Template - to accompany the EDPB Template. The reference open-source implementation provided with this Paper (see Part IV.7) includes such a pre-assessment as a first step to illustrate the feasibility of a single triage-to-notification flow.
This pre-assessment should also highlight mitigating factors which may lower a breach's severity (and the assessment effort) in a concrete case - for example, an availability-loss case where availability is promptly and fully restored; a ransomware which is quickly and fully undone by use of an up-to-date backup, or a wrong-recipient case where the recipient has confirmed deletion of the data - to help dissuade controllers from over-notifying where the residual risk for a breach is, in fact, low enough that no GDPR notification obligation arises. The reference implementation (Part IV.7) operationalises this as an explicit, non-exhaustive set of mitigating factors - credible confirmation of deletion from an unintended personal data recipient; the commonality or or homonymy of identifiers linked to an affected personal data set, reducing its identifiability; strong encryption applied to the affected data or other measures which render such data unintelligible to unauthorised recipients; professional secrecy obligations to which an unintended data recipient is bound; prompt and full restoration of data availability from backups; the already public or low-sensitivity nature of the affected data - which, when selected, create visible and editable adjustments to the relevant assessment variables (which are drawn from the ENISA methodology referred to in the next Section) This can allow controllers to show how each mitigating factor affects the severity assessment, in a manner consistent with the GDPR's principle of accountability.

I.4. Severity assessment: anchor the methodology field to ENISA (with a stated threshold)

While the EDPB Template asks controllers to "describe the methodology used and the relevant factors" (Field 90) and presents a three-level severity scale (Minor/Moderate/Severe), it **does not indicate a reference methodology**. This creates exposure to subjectivity (whether real or perceived) and inconsistency in assessments described across controllers.

As of the date of this Position Paper, the methodology for the assessment of severity of personal data breaches published by ENISA on 20 December 2013 (**"ENISA Severity Assessment**") is the *de facto* European standard for quantifying breach severity. Its core formula is

SE = DPC × EI + CB

where **DPC** is the "Data Processing Context", **EI** the "Ease of Identification" and **CB** the "Circumstances of the Breach":

- The DPC score reflects the criticality of the affected personal data (1 = "simple", 2 = "behavioural", 3 = "financial" and 4 = "sensitive");

- The EI score is a multiplicative correction addressing the ease with which affected data subjects may be identified from the relevant data - not an absolute value, but a factor to be modulated by the mitigating circumstances of the concrete case (for instance, a data subject's homonymy may make singling-out harder and therefore lower the EI; it is also true that this score is mostly relevant for confidentiality breaches, losing relevance for other types of breaches where personal data is not made available to unauthorised third parties); and

- The CB score adds to the final result considering the specific circumstances in which the breach occurred (for example, the number of unintended recipients in a confidentiality breach, the reversibility or lack thereof of undue data changes in an integrity breach and the temporary or definitive nature of data loss in an availability breach).

It allows for severity assessment results/severity scores within 4 bands: Low/Medium/High/Very High (ENISA Working Document v1.0, December 2013, developed by ENISA with the Greek and German DPAs - enisa.europa.eu/publications/dbn-severity; PDF: enisa.europa.eu/sites/default/files/publications/Data%20breach%20severity%20methodology_1.0.pdf).

Under this methodology, a severity score **below 2 corresponds to "Low"** - "[i]*ndividuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem* (…)" - whereas a score of 2 or above corresponds to "Medium" or above (described by ENISA as ranging from significant inconveniences to significant, or even irreversible, consequences for individuals). This SE >= 2/Medium threshold should be read as an indicative operational threshold rather than a normative cut-off point for GDPR notification obligations, given that ENISA's methodology does not supersede GDPR requirements, as well as that relevant risks to the rights and freedoms of natural persons under Article 33 GDPR may be absent even where a severity score equal to or greater than 2 is reached in a given case. As

such, this methodology can be used to support, but not replace, controllers' case-by-case legal assessments under Articles 33 and 34 GDPR.

Nevertheless, adding a recommendation for use of this methodology linked to Field 90 of the EDPB Template, in our view, incentivise controllers towards using it, with the consequence that they would be facilitated in generating reproducible and defensible results for their severity assessments, as would the relevant supervisory authorities be in scrutinising those assessments. This would, naturally, be without prejudice to the need for a case-by-case legal assessment of each breach under Articles 33 and 34 GDPR, as well as the possibility for controllers to apply other legally sustainable assessment methodologies.

This case-by-case modulation is not theoretical: the EDPB already applies it in its Guidelines 01/2021 on examples of breach notification, where the mitigating factors drive the outcome. In Case 1 (a ransomware attack with an intact backup, no exfiltration and data that remained encrypted) the residual risk is low and notification may not even be required, whereas in Case 3 (a ransomware attack on a hospital, with thousands of affected patients and postponed procedures, echoing real-world large-scale healthcare ransomware incidents in the EU) the risk is high and triggers both DPA notification and communication to data subjects. These mitigating factors map directly onto template fields 57 (data rendered unintelligible / encrypted) and 74-76 (security measures in place). [EDPB Guidelines 01/2021 on examples regarding personal data breach notification, adopted 14 December 2021: edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf].

To further facilitate use of the ENISA Severity Assessment in combination with the EDPB Template, an indicative mapping could be provided in connection with the severity levels currently listed in Field 87 of the EDPB Template and further adjustments could be made to allow controllers to directly submit ENISA Severity Assessment inputs (DPC, EI and CB scores) as structured fields within the EDPB Template and/or, potentially, even within the guided pre-assessment stage discussed in the previous Section. This standardisation could facilitate Member State and EU-wide analytics on notified personal data breach severity, which would, e.g., allow data-driven updates of regulatory guidance on personal data breach notification and management, increase cross-border consistency in application of Articles 33 and 34 GDPR and strengthen cooperation between EEA supervisory authorities - today, for various reasons, different supervisory authorities may reach different conclusions on equivalent incidents; a standardised, comparable severity input could reduce those divergences.

Proposal: Without mandating use of any given methodology:

1. Indicate the ENISA Severity Assessment as the recommended methodology in the Tooltip for Field 90 of the EDPB Template, flagging the “SE >= 2/Medium” indicative operational threshold (without prejudice to the need for controllers to carry out a case-by-case legal assessment under Articles 33 and 34 GDPR)

2. Provide an indicative mapping between the 4 ENISA Severity Assessment bands (Low/Medium/High/Very High) and the EDPB Template's 3 severity levels in Field 87 (e.g., Low → Minor; Medium → Moderate; High & Very High → Severe); and
3. Adjust the EDPB Template to allow controllers to submit the **ENISA Severity Assessment inputs (DPC, EI, CB) as structured fields**, so that a proposed severity score can be computed directly from the controller's declared inputs (noting that DPC, EI and CB scores remain qualitative judgments of the controller, not automated or objective risk assessments) in a manner comparable across notifications and supervisory authorities.

I.5. Misalignment of severity scales

The template uses **three levels** (Minor/Moderate/Severe), while ENISA uses **four** and many organisations use internal scales. Those already operating on ENISA or on four/five-level scales will have to remap, with a risk of lost granularity and inconsistency.

Proposal: clarify in the notes the relationship between the template's three levels and the commonly used scales, or consider adopting a four-level scale aligned with ENISA, the most widespread assessment tool.

I.6. Channel versus format

The EDPB Template harmonises notification **format**, not **channel**: notifications still must be addressed to the competent supervisory authority (for example, in Italy, the *Garante per la protezione dei Dati Personali,* via the online portal available at servizi.gpdp.it). The EDPB should **state clearly** that the EDPB Template does not establish a single European one-stop submission point to avoid creating the expectation that a centralised channel is created (a comparison between the EDPB Template and the Italian 2021 telematic breach notification tool, as well as those provided by other supervisory authorities, is set out in Part II of this Paper).

Part II - Comparison with international best practice and derived proposals

The EDPB Template can be adjusted to selectively absorb mature practices from other personal data breach notification procedures, each anchored to a verifiable primary source.

II.1 - Italy (*Garante per la Protezioni dei Dati Personali*): transition from a national form to the common template

Since 1 July 2021, the Italian supervisory authority (*Garante per la Protezioni dei Dati Personali*) has operated a structured telematic personal data breach notification procedure (following its decision of 27 May 2021 - https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9667201) as the sole

ordinary notification channel in Italy, with a preliminary/complete logic and automatic reminders. - a similar mechanism to that used by the EDPB Template for complete/incomplete/follow-up notifications. Italy was, therefore, already ahead, and the step for Italian controllers to adapt to the EDPB Template will be modest ; (servizi.gpdp.it/databreach).

Italy is not an isolated case in the EEA. Several supervisory authorities have been operating dedicated national breach notification channels before the EDPB Template was published. As a result, the EDPB Template appears to largely harmonise pre-existing national practice rather than create it *ex novo*.

In Portugal, the *Comissão Nacional de Proteção de Dados* makes an online form for personal data breach notification available to controllers (https://www.cnpd.pt/databreach/?AspxAutoDetectCookieSupport=1), which also allows for the submission of initial notifications and updates to previously submitted notifications, as does the online form made available by the *Commission Nationale de l'Informatique et des Libertés* in France (cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles), with the added benefit that this form can be saved and completed in stages. The Spanish (*Agencia Española de Protección de Datos*), Dutch (*Autoriteit Persoonsgegevens*) and Irish (Data Protection Commission) supervisory authorities likewise provide dedicated pre-existing national notification portals (EDPB hub, 'How to notify a data breach to your DPA': edpb.europa.eu/notify-data-breach_en). The EDPB Template's preliminary/complete logic therefore codifies a converging practice already established in the most active jurisdictions.

Observation: While the EDPB Template harmonises notification format, supervisory authorities which already have their own notification tools will need a transition phase to adapt to the EDPB Template. The EDPB should, arguably, indicate a timeline and a coexistence period to avoid misalignment between the new format set by the EDPB Template and existing national portals.

II.2 - UK (ICO): the guided self-assessment

The ICO integrates a **self-assessment decision tree** guiding the "notify or not" decision (is it a personal data breach? → is there a risk? → report to the ICO? → inform the data subjects? → document), plus published examples and an above/below-threshold distinction (ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/).

This is the source of the pre-assessment proposal in Part I.3 of this Paper.

II.3 - Australia (OAIC) and Singapore (PDPC): individual-facing/confidential separation and clear triggers

- **The Office of the Australian Information Commissioner (Australia)** uses a **two-part form**: Part 1 (statement) holds the information that must also be communicated to individuals, and Part 2 - optional - may be kept confidential by the regulator. This creates an explicit separation between information shared with affected individuals and confidential information toward the authority (oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach).
- **The Personal Data Protection Commission (Singapore)** uses an **explicit dual notification threshold**: significant harm OR a numeric scale (≥500 affected individuals) (pdpc.gov.sg/report-data-breach).

The EDPB Template does not clearly identify whether specific fields are also to be communicated to data subjects (in the event that Article 34 GDPR applies), as opposed to being fully reserved to the competent supervisory authority. Doing so could help make the EDPB Template usable also, at least in part, for communications to data subjects required under Article 34 GDPR, which would reduce the associated burden on controllers.

Proposal (OAIC): Adopt a **two-tier structure for the EDPB Template based on the OAIC model** - a set of core Fields marked as "communicatable to data subjects" and a "reserved to the supervisory authority" tier.

II.4 - USA (California AG, FTC HBNR): transparency and sectoral models

- **California Attorney-General**: Organisations communicating a relevant incident to more than 500 California residents must send a sample of the communication to the AG, which maintains a **public, searchable database** of such communications and provides an official template for such communications (oag.ca.gov/privacy/databreach/list).
- **Federal Trade Commission Health Breach Notification Rule** (16 CFR Part 318): a sectoral model for health data outside HIPAA (PHR vendors, health apps), relevant to the EHDS/wearables interface. [ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0].

Developing a concrete personal data breach notification transparency model to accompany the EDPB Template, modelled after the database maintained by the California AG, could [benefits]. This model would be made publicly available, subject to periodic updates. It would aggregate data collected from notifications submitted using the EDPB Template and display it in a defined subset of structured fields - for example:

- Breach Nature (drawing from the EDPB Template's breach nature taxonomy);
- Cause (drawing from the EDPB Template's quadrant: internal/external x

malicious/non-malicious);

- Affected Personal Data Categories;
- Affected Data Subjects (bracketed into ranges rather than exact figures);
- Severity Level;
- Whether Article 34 GDPR communication was required.

To preserve anonymity of notifications towards the general public, the reported data should not focus on the level of individual notifications, instead presenting data drawn from relevant submissions over a given reporting period (e.g., quarterly or annually). Controller identity should not be disclosed, data from EDPB Template free-text fields should not be used and small-cell suppression/k-anonymity should be deployed as relevant (e.g., by not reporting any data on a given field where less than 5 submissions were made during a relevant reporting period). In particular, aggregate publications should carry no dates finer than the reporting period (for example, the quarter), so that individual incidents cannot be re-identified through the timing of their publication.

Because every reported field would be drawn from the EDPB Template's controlled vocabulary, the presented statistics would be comparable across supervisory authorities by design. This could allow for the creation of a pan-European evidence base for transparency and research on personal data breach notifications.

A reference schema for such an aggregate model is included with the technical annex to this Position Paper (Part IV.7).

Proposal (California) [concrete model]: Accompany the EDPB Template with a concrete transparency model - a periodically published, aggregate and anonymised statistical dataset of notifications, derived directly from the template's controlled vocabulary.

II.5 - Canada (OPC/PIPEDA): record-keeping of all breaches

The Canadian regime (Breach of Security Safeguards Regulations, **SOR/2018-64**) requires **mandatory record-keeping of ALL breaches** - including those below the notification threshold ("Real Risk of Significant Harm"). Records should be retained for a minimum of 36 months from the day the organisation determines the breach occurred, with detail sufficient to allow the authority to verify that the risk was properly assessed (laws-lois.justice.gc.ca/eng/regulations/SOR-2018-64/index.html; Office of the Privacy Commissioner of Canada guidance: priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/).

Article 33(5) GDPR already requires controllers to document all personal data breaches (including those not notified), but in generic terms (the EDPB's own Guidelines 9/2022, footnote 47, confirm that a separate register is not required where the information is

identifiable and can be extracted on request; what follows is therefore offered as an optional, standardised form, not as a gap to be filled). The EDPB could **give operational shape to the Article 33(5) GDPR documentation duty taking inspiration from the Canadian record-keeping model** by, alongside the EDPB Template, providing a template Personal Data Breach Register aligned with the EDPB Template's fields. Relevant fields could include, for example:

- Incident reference and date (or period): Fields 7 & 44 to 48;
- Nature (C-I-A): Field 55;
- Circumstances and cause of the breach (if known): Fields 60 to 62;
- Affected data subject categories and approximate numbers: Fields 65 to 68;
- Affected personal data categories and approximate record numbers: Fields 70 to 73;
- Risk-assessment outcome and methodology, including where the conclusion was "no high risk": Fields 89 & 90;
- Measures taken: Fields 92, 94 & 95;
- Whether notified to data subjects and/or to the supervisory authority (and, if not, the reasoned basis): Fields 97 to 103.

On retention, the EDPB could suggest a minimum period - as guidance and certainty for controllers rather than as an obligation - while making clear that the period ultimately remains for each controller to determine on accountability grounds. This is consistent with the EDPB's own Guidelines 9/2022 (para 124): the GDPR fixes no retention term, and the operative criterion is evidentiary - a controller should retain for as long as it may be called upon to demonstrate that it handled the breach lawfully. We suggest a minimum of 36 months from the date the controller became aware of the breach, stated plainly as a declared floor rather than a measure of full coverage, because the evidentiary window is in fact typically longer: Article 82(6) GDPR, through Article 79(2), opens two alternative fora - the controller's establishment or each data subject's residence - so a controller with data subjects in several Member States may face litigation in more than one of them and should weigh the outer envelope of limitation periods potentially engaged by the available fora and the applicable-law analysis, rather than any single national term; the duration of any ensuing litigation is then added rather than substituted (in Italy alone, by way of illustration: five years for administrative sanctions and their collection under Article 28 of Law 689/1981; five years for tort claims under Article 2947 of the Civil Code, extendable where the same fact is a criminal offence carrying a longer term under Article 2947(3); and ten years for contractual claims under Article 2946). A controller with greater exposure should therefore retain for longer than the suggested minimum. The 36-month period would accordingly not operate as a safe harbour: at the expiry of that baseline, a controller should run and document a jurisdiction- and exposure-specific retention assessment. A two-layer distinction makes this workable and answers the anonymity question directly: the register in the strict sense - incident categories, approximate counts, nature, risk-assessment outcome and measures (the fields listed above), mirroring what Article 33(3)(a) already frames in categories and approximate numbers - can be held in a form that contains no personal data, in which case the GDPR's storage-limitation principle does not apply, though the register remains subject to ordinary governance and record-management

choices. It is precisely for that reason that such a register should be kept deliberately lean: anonymity under Recital 26 is relational (singling-out remains possible without names) and is assessed in light of technological developments, so the longer a record is retained the more a rich, case-by-case description erodes its own anonymity. This assessment is given operational shape by the EDPB's draft Guidelines 02/2026 on anonymisation (Version 1.0, adopted for public consultation on 7 July 2026 and open until 30 October 2026, and therefore not a settled position): they translate the Recital 26 principle into three cumulative 'safe-pass' criteria - no record isolation, no linkage and no inference - which, if all passed under the chosen approach, allow the data to be safely considered anonymous, whereas the failure of one triggers further analysis rather than an automatic finding of personal data; and, more broadly than a reading limited to the controller and third parties, they confirm that the parties able to identify an individual may, depending on the circumstances and the access and security context, include unauthorised and malicious actors, which for a breach register retained for years supports a conservative assessment rather than lowering the bar. For a register intended to be retained for years we would suggest the more conservative 'simplified' approach of those Guidelines, stated openly as a prudential choice and not as an alternative legal standard or a settled legal reading. The same draft also draws the consequence that the likelihood of re-identification tends to increase over time, so that data once anonymous should again be considered personal - re-engaging GDPR obligations and accountability for any processing from that point onward - and recommends periodic reassessment of that likelihood. Our recommendation is therefore not a fixed retention figure but a mechanism: a lean, genuinely anonymous register, kept under periodic re-identification review, may be retained for as long as it remains anonymous; this converges operationally with the ICO's approach to breach logs containing personal information (set a period, justify it, review it periodically, and reduce personal information where possible). We offer this as coherent with the direction of that open consultation, which is also the natural venue in which to develop it. Pseudonymisation does not suffice here - pseudonymised data remain personal data, and the storage-limitation principle continues to apply. The case file proper - lists of affected data subjects, any Article 34 communications, related correspondence - does contain personal data and remains subject to the ordinary retention analysis. Finally, the EDPB's own paras 122 and 124 already tie this documentation's evidentiary value to accountability generally, not only to Article 33, which widens what the record should be capable of evidencing for accountability purposes, without introducing any requirement that the record identify individuals.

Doing so would help controllers strengthen their accountability towards personal data breaches and potentially reduce defensive notifications (allowing controllers to more confidently document low-risk breaches internally rather than notifying them as a precaution).
The reference implementation included with this Paper (Part IV.7) includes a downloadable internal-register model (CSV / XLS export) that implements relevant fields from the EDPB Template, which could be directly adopted by controllers to support in compliance with Article 33(5) GDPR requirements..

Proposal (Canada) [NEW, strong]: Alongside the EDPB Template, provide a template Personal Data Breach Register aligned with the EDPB Template and in line with Article 33(5) GDPR.

II.6 - International standards: aligning with ISO/IEC 27035

The **ISO/IEC 27035-1:2023** standard (information security incident management - principles and process) defines a recognised incident-management **lifecycle and vocabulary**: Plan & Prepare → Detect → Report → Assess → Respond → Learn Lessons (iso.org/standard/78973.html - ISO/IEC 27035-1:2023). It does not, however, provide a taxonomy of breach nature types equivalent to that provided by the EDPB Template. The value in drawing from this standard is, therefore, focused around **process and terminology alignment**.

By referencing this standard as the interoperability anchor for personal data breach/incident lifecycle and vocabulary in the EDPB Template, controllers' internal incident management processes - frequently already aligned with ISO 27035 - can provide relevant input to the EDPB Template for GDPR notification without needing to first undertake a parallel re-classification exercise to ensure consistency in used vocabulary. This point is best framed as promoting interoperability and machine-readability, in that a controller's existing security-operations terminology should map cleanly onto the notification created through the EDPB Template for this to work as intended *(Note: the full normative text of ISO/IEC 27035 is paywalled; references should cite the standard by number and clause without reproducing protected text).* The EDPB Template's notification stages (initial / follow-up / final) can be aligned with the ISO/IEC 27035 phases (detection, assessment, response, lessons learnt); on vocabulary, the Template's controlled incident-nature taxonomy can in turn be mapped to ISO/IEC 27035 terminology, as an illustrative alignment.

Proposal (ISO): the EDPB could reference ISO/IEC 27035 as the interoperability anchor for the EDPB Template's incident lifecycle and vocabulary., so that a controller's internal incident-management process - frequently already ISO 27035 / ISO 27001-aligned - feeds the GDPR notification without a parallel re-classification. The point is best framed as interoperability and machine-readability (a controller's existing security-operations terminology should map cleanly onto the notification), rather than as a literal type-for-type correspondence. *(The full normative text of ISO/IEC 27035 is paywalled; references should cite the standard by number and clause without reproducing protected text.)*

II.7 - Comparative value summary

The template, already solid, can selectively absorb four mature best practices: individual-facing/confidential separation (OAIC), guided self-assessment (ICO), the link to the internal Article 33(5) record (Canada), and the anchoring of the taxonomy to an international standard (ISO 27035). These are incremental enhancements, not rewrites, all consistent with the current design.

Part III - EDPB Template section-by-section comments

Section 1 - Notification type

- **Formal withdrawal** of a notification: a positive novelty (duplicate, or risk excluded after assessment). *Proposal*: add a structured field for the withdrawal reason (duplicate / risk reassessed as unlikely / filing error), useful for statistics and accountability.

Section 2 - Controller and notifier

- The dedicated **processor / joint-controller** field is welcome. *Proposal*: add a flag indicating whether the breach was detected by the processor and notified to the controller under Article 33(2), with the relevant date, to reconstruct the awareness chain relevant to the 72-hour clock.
- The reporting person and responsibility for accuracy (fields 23 and 26). The template allows the reporting person to be the DPO: field 23 ("Function of the reporting person") lists the DPO as the first option, alongside the legal representative and the authorised representative. Within the same section, field 26 ("Accuracy & Responsibility") provides, as an optional field to be implemented only if required, the "information on the liability for the accuracy of the information provided (can be combined with Art. 13 information)", yet with no standard wording: the content of the accuracy statement is left entirely to the implementation of each Authority. Where an Authority implements the field and the reporting person is the DPO, the accuracy statement formally attaches to the submission made by the DPO, whereas the notification obligation and the responsibility for its content rest with the controller (Articles 33(1) and 24 GDPR), the DPO is a contact point (Article 33(3)(b)) and is not personally responsible for compliance (WP243 Guidelines). Having the DPO attest to accuracy would moreover create a tension with the DPO's independence: the DPO would be attesting to facts on which they are required to advise and monitor (Article 39(1)(a)-(b)), with a potential conflict of interests (Article 38(6)) and a risk of indirect pressure incompatible with Article 38(3). As an optional field with no common formula, absent a standard EDPB wording each Authority may frame the statement differently, leading to divergent practices across Member States, against the harmonising purpose of the template. Proposal: accompany field 26 with a standard formula and an explanatory note (a tooltip in Authority portals) along the following lines: "The reporting person submits the notification on behalf of the controller; responsibility for the accuracy and completeness of the information provided remains with the controller (Articles 24 and 33(1) GDPR)". The formula clarifies the reporting person's material transmission role, preserves the DPO's independence where the DPO acts as reporting person, remains combinable with the Article 13 information as the field already contemplates, and harmonises implementation across Authorities.

Section 3 - Initial breach information

- The **delay-justification field auto-triggered beyond 72h** is an excellent embedding of Article 33(1). *Caution*: ensure the clock starts from the controller's "awareness", not the date of the breach, and that the field handles phased (preliminary) notification without penalising those who notify promptly but incompletely.
- The **C-I-A triad with sub-qualifications** (e.g. confidentiality: exfiltrated / likely exfiltrated / not exfiltrated with evidence) is solid and consistent with Guidelines 9/2022.
- The **encryption/intelligibility field** with an intermediate "measures present but likely circumventable" option is realistic and useful. *Proposal*: explicitly connect this field to the Article 34(3)(a) exemption in the conditional logic, so that a declaration of effective encryption pre-fills/orients Section 5 on communication to data subjects.
- **Data-subject categories with flags for minors and vulnerable persons**: welcome, consistent with Recital 75.

Section 4 - Further information (the assessment core)

- Severity + risk-assessment outcome fields: see Sections 4-5 of Part I. *Proposal*: make explicit in the form the link between the risk-assessment outcome (high risk / risk / unlikely risk) and the obligations that follow (Article 33 notification to the DPA / Article 34 communication to data subjects), with contextual guidance. Multi-value fields: the template appears to permit multiple selections explicitly on only one field, while several enumerated fields are inherently multi-valued. A single breach commonly affects more than one nature dimension (confidentiality, integrity and availability can be compromised together - the template itself provides separate C/I/A sub-types), more than one category of personal data and of data subjects (Article 33(3)(a) refers to "categories" in the plural), and entails several likely consequences and several security and remediation measures. Forcing a single choice on these fields loses information, distorts the controller's description and undermines the comparability of aggregate statistics. Proposal: the EDPB should explicitly enable multiple selection on the fields that are inherently multi-valued - in particular the nature of the breach (C/I/A), the categories of personal data and of data subjects, the likely consequences and the measures in place or proposed - while keeping single selection where a single primary value is appropriate (notably the primary incident type, to preserve the statistical comparability of the 25-type taxonomy). The reference implementation flags these fields as multi-valued (multi-select).

Section 5 - Communication to data subjects

- The **Article 34(3) exemptions as structured options** are excellent codification. *Proposal: for exemption (c) (disproportionate effort → public communication), add a field describing the public-communication method adopted, to support accountability. The EDPB could go further and indicate in advance the acceptable modalities of public*

communication - for example a dedicated FAQ or notice published on the controller's website - so that controllers relying on exemption (c) have a clear and harmonised reference.

Section 6 - Other aspects (cross-border, other authorities)

- The **interaction with NIS / other authorities** field is useful and timely, given the growing overlap between GDPR notifications and NIS2/DORA notifications for the same incident. *Proposal*: include an explicit reference to coordination with notifications due to other authorities for the same event (NIS2, DORA, sectoral authorities), to reduce duplicated effort and signal the plurality of obligations. **Timeline interoperability with NIS2**: GDPR uses a single 72-hour notification, whereas NIS2 (Article 23) uses a staged 24-hour early warning → 72-hour notification → one-month final report. The template already supports preliminary/complete/follow-up sub-types (fields 3-4); the EDPB could explicitly **map these sub-types onto the NIS2 staging**, so an entity in scope of both files a coherent, non-duplicative sequence - a concrete SME-relief measure. [NIS2 Dir. (EU) 2022/2555, Art. 23: eur-lex.europa.eu/eli/dir/2022/2555/oj]. A parallel staged regime exists under DORA for major ICT-related incidents (Article 19 of Regulation (EU) 2022/2554): an initial notification within 4 hours of classification as major (and within 24 hours of awareness), an intermediate report within 72 hours, and a final report within one month (RTS (EU) 2025/301 and ITS (EU) 2024/2956). For an entity in scope of both GDPR and DORA, a single personal-data breach occurring within an ICT incident can trigger two parallel reporting tracks with different timelines and taxonomies; mapping the template's preliminary/complete/follow-up sub-types onto these staged regimes would reduce misaligned double reporting. This alignment is specific to entities in scope of both regimes - DORA is sectoral, applying to financial entities - and is not a general rule.
- **Non-EEA controllers without an establishment** (Article 3(2) GDPR): the need to notify every DPA of the countries where data subjects are located, absent a one-stop-shop, remains a significant burden. The template handles it well by including the DPA list, but the underlying fragmentation is a systemic matter beyond the template. The doctrinal basis for these extra-EEA fields (around 119-123) is paragraph 73 of the EDPB Guidelines 9/2022 on personal data breach notification (v2.0), whose key update concerns precisely the notification obligations for breaches at establishments outside the EU: a non-EEA controller without a main establishment must notify each supervisory authority concerned. [EDPB Guidelines 9/2022 v2.0, para 73: edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf] (Developed in Part II.)

Section 7 - Attachments

- The typed attachment list (copy of the communication to data subjects, risk assessment, ransomware note, phishing message) is practical and useful to

investigations. *Proposal*: add guidance on accepted format and maximum size, to avoid divergence across DPA implementations.

Part IV - Machine-readable standardisation and an optional M2M channel

In its 1.0 version the template is in fact already a **structured electronic module with conditional logic**, meant for implementation in DPA portals. This opens an opportunity the current Word document does not yet exploit: standardising not only the visual form, but the data format and the transmission channel. A note on how to read this paper: the contributions fall into three tiers - (A) essential observations on the template itself (Parts I-III); (B) optional technical proposals that the EDPB and the DPAs may take up at their discretion (this Part IV.1 to IV.6); and (C) a non-binding technical annex (Part IV.7). The optional and forward-looking items are deliberately kept separate from the essential observations, so that the core consultation feedback can be read on its own.

IV.1 - The proposal

Pair the form with two open technical artefacts:

1. A **machine-readable schema** (a JSON Schema of the fields): it formalises, unambiguously, the structure, data types, conditional logic and constraints. The schema becomes the "contract" of the format, identical across the EU.
2. A **receiving API endpoint (OpenAPI 3.1)** for automated machine-to-machine (M2M) transmission of notifications from organisations to DPAs: undertakings with incident-management systems (SIEM/SOC, privacy GRC tools) could notify directly from their tools rather than re-keying a form manually.

IV.2 - Policy arguments

- **Timeliness (Article 33(1))**: automated transmission reduces transcription errors and speeds compliance with the 72-hour deadline by removing the manual re-entry of data already held in corporate systems.
- **Real cross-border interoperability**: an identical payload can be addressed to the lead supervisory authority (Article 56 GDPR) or, for non-EEA controllers, to several DPAs at once - operationally overcoming the fragmentation that today forces different forms in different languages. It is the technical translation of the template's cross-border section.
- **Consistency with the current design**: the embedded conditional logic already makes the template an electronic module; the machine-readable schema is its natural formalisation, not an external addition.
- **A consolidated EU trend**: structured machine-readable reporting to authorities is already the direction of EU legislation - see the structured templates for major

ICT-incident reporting under DORA and the multi-stage notifications under NIS2. An M2M channel for GDPR breach notifications fits this path; it is not an outlier.

- **National precedent**: the Italian Garante has had a telematic channel since 2021 (docweb 9667201). Several other DPAs likewise operated dedicated breach-notification channels before the template: France's CNIL uses the same two-phase logic (an initial 72-hour notification followed by a supplementary one), while Spain (AEPD), the Netherlands (AP) and Ireland (DPC) provide pre-existing dedicated national portals (EDPB hub, 'How to notify a data breach to your DPA') - so a machine-readable channel builds on an established practice rather than introducing a wholly new one. The API would be its natural evolution.

IV.3 - Voluntariness and proportionality

The M2M channel is to be understood as an **option, not a replacement for the web form**. SMEs without automated systems continue with the form; organisations with a SOC/GRC tool use M2M. The proposal is therefore consistent and complementary with the "SME track" (Part I, Section 2): no additional burden on less-structured entities. These artefacts are offered as soft-harmonisation instruments: the EDPB can recommend a template and issue guidance, and can make a reference schema and API available, but whether to adopt a common machine-readable schema or an M2M channel rests with the EDPB's and the DPAs' own assessment of their competence and legal basis. The technical proposals in this Part are therefore offered, not imposed.

IV.4 - Security of the channel (Article 32 by design)

An endpoint receiving breach notifications itself processes personal data and sensitive security information: it must therefore be **itself compliant with Article 32 GDPR**, so as not to become a new risk vector. The proposal is security-by-design, with the following measures (already specified as requirements in the OpenAPI specification):

#	Measure	Function
1	**TLS 1.3 + mTLS** (mutual TLS)	Encrypted transport; both the sending organisation and the DPA authenticate with certificates
2	**OAuth 2.0 client credentials** (short-lived, scoped token) + mTLS	Defence in depth; the controller/DPO identity in the payload is bound to the authenticated client (mapped to a registered controller), preventing spoofed notifications
3	**Request signing - JWS / HTTP Message Signatures (RFC 9421)**	Integrity and **non-repudiation**: the DPA can prove WHO sent the notification and that the payload was not altered. Legally crucial: a

#	Measure	Function
		breach notification is a legal act with a 72-hour deadline
4	**Idempotency-key**	Avoids duplicates on retransmission (network failure during the 72 hours); ties into the template's follow-up/withdrawal logic
5	**Per-client rate limiting**	The endpoint must not become a DoS vector
6	**Immutable audit log** (sender, timestamp, payload hash)	Article 32 + Article 5(2) accountability
7	**Server-side validation against the JSON Schema**	Malformed payloads rejected; the schema is the contract
8	**API versioning**	Schema evolution without breaking clients

Point 3 (cryptographic non-repudiation) deserves legal emphasis: by turning the notification into a signed message with proof of sender and timestamp, the API strengthens certainty of compliance with the 72-hour deadline - a benefit both for the controller (proof of timeliness) and for the DPA (proof of authenticity).

IV.5 - Forward-compatibility with the Digital Omnibus single reporting entry point

The Digital Omnibus proposes an ENISA-operated single entry point ('report once, share many') routing incident and breach notifications across NIS2, GDPR, DORA, eIDAS and CER: the entity notifies once, and the back-end routes the submission to the relevant authorities. The single entry point is part of the broader Digital Omnibus package: introducing a proposed new Article 23a of the NIS2 Directive and an ENISA-operated entry point. It is still under the ordinary legislative procedure, with adoption expected in the course of 2026; if adopted, the single entry point would become available approximately 18 months after the new measures enter into force (extendable to 24 months if the EU Commission finds the portal does not yet meet the required integrity, reliability and confidentiality standards). The EDPB breach template could/should be designed **upfront** to be compatible with that single-entry-point data model, so that one structured submission can satisfy multiple regimes. This turns the template from a GDPR silo into the GDPR node of a pan-regulatory reporting fabric - aligning with the EU Commission's own simplification agenda.

Important framing: the single entry point is, at the time of writing, a European Commission proposal (19 November 2025) still under the ordinary legislative procedure, with adoption expected in the course of 2026. It is not yet adopted law (and is distinct from the 'Digital

Omnibus on AI' file, which the European Parliament approved on 16 June 2026). This recommendation is therefore made strictly as forward-compatibility / anticipation of a proposal in progress, not as compliance with an existing obligation.

Proposal: ensure the template's data model (field names, controlled vocabulary, identifiers) is designed to be forward-compatible with the single-entry-point schema envisaged by the Digital Omnibus proposal, so that - if and when adopted - the GDPR notification can be emitted or consumed by the common entry point without re-mapping. [EDPB-EDPS Joint Opinion 2/2026 on the Digital Omnibus: edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf ; NIS2 Art. 23: eur-lex.europa.eu/eli/dir/2022/2555/oj].

IV.6 - Multilingual consistency of the controlled vocabulary

With +27 DPAs implementing the template, the enumerations (incident types, data categories, exemptions) must be **semantically identical across languages**, to avoid a "same field, different meaning" drift between national portals.

Proposal: the EDPB should maintain the controlled vocabulary centrally with **stable, language-independent keys**, binding translations to those keys. The reference schema (IV.7) already implements this: the enumerations use stable semantic keys (e.g. loss_of_confidentiality, or letter codes a/b/c) so that the **transmitted value is identical across all EU languages** - only the displayed label changes, never the value. Two DPAs operating in different languages therefore receive the same payload. This is the technical foundation of multilingual consistency, and it links the multilingual-consistency, single-entry-point and machine-readability objectives.

IV.7 - Reference implementation (annex)

To make the proposal concrete, a first reference implementation is annexed to this paper as a non-binding technical contribution released under CC BY 4.0:

- A **JSON Schema (Draft 2020-12)** of the notification payload derived from template v1.0: **100 input fields** (of 126 total rows, 26 being section/structure), of which 42 always mandatory, 46 conditional and 12 optional.
- **Complete taxonomies faithfully reproduced**: 25 incident types, 21 data categories (a-u), 6 causes, 3 severity levels, 3 Article 34(3) GDPR exemptions, the C-I-A triad, NACE classification, complete EEA supervisory-authority lists. 90 of 100 fields are anchored to specific GDPR articles.
- **Conditional logic** (visible_if / required_if) transcribed in full from the template's "business logic" column.
- A guided pre-assessment step (Part I, Section 3), an ISO/IEC 27035 mapping of the incident taxonomy (Part II.6), a downloadable Article 33(5) breach-register model (CSV / XLS export) implementing the fields proposed in Part II.5, and an aggregate,

anonymised transparency-statistics schema (Part II.4) with small-cell suppression (k >= 5).

Method: cell-level extraction from the native table of the official .docx file, with two independent parses and diff reconciliation (zero cell-boundary ambiguity). The OpenAPI 3.1 specification, with the securitySchemes at IV.4, is complete (OpenAPI 3.1.0, mTLS and OAuth2 security schemes, the eight Article 32 measures of Section IV.4 documented, validated against a tested mock server) and will be released on the same terms upon publication.

Reference implementation and technical artefacts (CC BY 4.0)

Repository: https://github.com/NicklawAI/edpb-breach-notification-assistant
Landing page: https://nicklawai.github.io/edpb-breach-notification-assistant/
Offline tool: https://nicklawai.github.io/edpb-breach-notification-assistant/tool.html
JSON Schema:
https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/src/schema/breach-notification.schema.json
OpenAPI 3.1:
https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/api/openapi.yaml
Article 33(5) breach-register example:
https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/paper/breach-register.example.csv
Aggregate-transparency example
https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/paper/aggregate-transparency.example.json .

Caveat: the schema is a technical interoperability reference, not a submission channel - the template remains under consultation and is not usable for real notifications until DPAs implement it.

GDPR field-to-article map (inline):

GDPR article	Fields	Theme
Art. 4(12); Art. 33(3)(a)	55	Definition and nature of the breach
Art. 33(1)	44-53	Timeline and 72h deadline (awareness/detection)
Art. 33(2); Art. 28; Art. 26	38-41	Processor / joint-controller involvement
Art. 33(3)(a)	10-19, 21-26,	Controller identity + data-subject/record categories and numbers

GDPR article	Fields	Theme
	56-63, 65-68, 70-73	
Art. 33(3)(b)	29-31, 33-36	DPO / contact point
Art. 33(3)(c)	79-87	Likely consequences and severity
Art. 33(3)(d)	92, 94-95	Measures taken / proposed / preventive
Art. 32; Art. 33(3)	75-76	Security measures in place
Art. 33(1); Art. 34(1)	89-90	Risk assessment / high-risk threshold
Art. 34(1); Art. 34(2)	97-99, 102-106	Communication to data subjects
Art. 34(3)(a)(b)(c)	100-101	Exemptions from communication to data subjects
Art. 56	113-118	Cross-border processing / lead SA (one-stop-shop)
Art. 3(2)	120-123	Non-EEA controller / extraterritoriality

Part V - Summary of proposals

From general and field comments (Parts I-II):

1. Introduce a simplified "SME track" based on the Article 33(3) minimum.
2. Anchor field 90 to ENISA SEV (SE = DPC x EI + CB; SE >= 2 as an indicative operational threshold, without prejudice to the case-by-case assessment under Articles 33 and 34) + indicative level mapping; let the computed value pre-populate the template.
3. Clarify/align the severity scale (3 vs 4 levels).
4. Clarify that the template harmonises the format, not the channel (no single submission point).
5. Structured reason field for notification withdrawal.
6. Flag and date of the processor→controller notification under Article 33(2).
7. Connect, in the conditional logic, the encryption field to the Article 34(3)(a) exemption.
8. Explicit reference to coordination with NIS2/DORA/other-authority notifications.
9. Guidance on attachment format/size.

From the international comparison (Part II):

10. A two-tier structure (an individual-facing statement plus optional regulator-confidential information) on the OAIC (Australia) model, so the template also serves the Article 34 communication.
11. 11. A guided "notify or not" pre-assessment upstream, on the ICO (UK) model, to reduce defensive notifications.
12. A link to the internal breach register under Article 33(5) GDPR on the Canadian record-keeping model, with a model structure aligned with the template's fields.
13. Align the incident vocabulary and lifecycle with ISO/IEC 27035 (process/terminology interoperability, not a literal type mapping).
14. [concrete model] Propose a concrete aggregate, anonymised transparency model on the California model, derived from the template's controlled vocabulary (incident type, cause, data categories, severity band, sector, bracketed data-subject counts, Article 34 flag), at category-count granularity per reporting period, with small-cell suppression / k-anonymity guarantees (recommended minimum k >= 5) and a reference schema in the annex, turning the taxonomy into a comparable pan-European evidence base.
15. Indicate a timeline and a coexistence period for the transition from existing national forms (e.g. the Italian 2021 tool).

Technical proposal (Part IV):

16. Standardise the data format (JSON Schema) and an optional M2M API channel for automated transmission from corporate systems to DPAs - security-by-design (mTLS, OAuth2, JWS non-repudiation, immutable audit), voluntary and complementary to the form for SMEs, consistent with the DORA/NIS2 trend. A reference open-source implementation is available as a technical contribution under CC BY 4.0.
17. **[forward-looking - proposal not yet adopted]** Design the template forward-compatibly with the Digital Omnibus single reporting entry point (one structured submission serving NIS2/GDPR/DORA/eIDAS/CER). NB: the single reporting entry point is a European Commission proposal (a proposed Article 23a NIS2, 19 November 2025) still under the ordinary legislative procedure, with adoption expected in the course of 2026; framed here as anticipation, not existing law.
18. **[forward-looking]** Map the template's preliminary/complete/follow-up sub-types onto the NIS2 staged timeline (24h/72h/1-month) for non-duplicative multi-regime reporting.
19. Allow a proposed severity band to be computed from the controller's declared ENISA inputs (DPC/EI/CB) - a qualitative judgment of the controller, not an automated risk assessment - for cross-DPA comparability and EDPB analytics.
20. Maintain the controlled vocabulary centrally with stable, language-independent keys to ensure multilingual consistency across 27+ DPAs.
21. Enable multiple-selection (multi-value) cardinality on the inherently multi-valued fields - nature of the breach (C/I/A), categories of personal data and of data subjects, likely consequences, and measures in place/proposed - keeping single-selection for the

primary incident type to preserve taxonomy comparability. The reference implementation already flags these fields as multi-valued (multi-select).

Part VI - Licence and free adoption

This position paper and its technical annexes (JSON Schema, field catalogue, ISO/IEC 27035 mapping, OpenAPI specification, and the guided pre-assessment) are released under the **Creative Commons Attribution 4.0 International Licence (CC BY 4.0)**.

The artefacts are made available for adoption by the EDPB, the national Data Protection Authorities and any EU institution, with no restriction beyond attribution. Under CC BY 4.0, DPAs are free to adopt, adapt, implement and redistribute the schema, the mapping tables and the reference implementation, including in their own portals. The artefacts are available in the public repository (https://github.com/NicklawAI/edpb-breach-notification-assistant); Stakeholders have adhered and will keep adhering via the repository's adherence form (https://github.com/NicklawAI/edpb-breach-notification-assistant/issues/new?template=adhere.yml), with signatories listed at https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/SIGNATORIES.md The processing of signatories' personal data is described in the privacy notice (https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/PRIVACY.md; IT version: https://github.com/NicklawAI/edpb-breach-notification-assistant/blob/main/PRIVACY.it.md).

4 August 2026

Nicola Franchetto LL.M

Martim Taborda Barata