DOT Europe consultation response

Public consultation on the EDPB draft template for personal data breach notification

---

Introduction

DOT Europe welcomes the opportunity to comment on the European Data Protection Board's ("EDPB") draft template for personal data breach notification under Article 33 GDPR.

We support the EDPB's objective of harmonising breach notifications across the Union and of providing organisations, in particular smaller ones without dedicated compliance teams, with a clear and predictable format to report incidents. A well-designed, genuinely proportionate template can reduce legal uncertainty for controllers and improve the quality and comparability of the information reaching supervisory authorities.

As drafted, however, the template goes beyond what Article 33(3) GDPR requires. At a time when EU institutions are actively pursuing regulatory simplification, including through the ongoing Digital Omnibus proposal, which would itself amend core elements of the Article 33 notification duty, we believe the template should be revised to ensure adequate reporting while, where possible, reduce reporting burden on companies. We set out below our overarching concerns, followed by comments on specific fields, and conclude with observations on how the template should be aligned with other EU legal instruments.

Overarching Concerns

1. A disproportionately long and detailed template

The template proposes close to 100 information fields, which considerably exceeds the four elements that Article 33(3) GDPR requires a notification to contain. By comparison, the existing recommended templates used in France, Spain and Ireland are approximately one third of the length of the EDPB's proposal. The template also contradicts the EDPB's commitment under the Helsinki statement to 'facilitate easier GDPR compliance'. Regulators should be making it easier for organizations engaging in good faith to make additional transparent disclosures while minimizing administrative complexity. At a time when EU industry is voicing concern about regulatory burden and policymakers are actively considering simplification, increasing the length and duration of breach notification beyond current practice does not appear proportionate.

We would encourage the EDPB to revisit the exercise so that the resulting burden remains reasonable and workable for all controllers, including SMEs, particularly given the short statutory deadline within which a notification must be filed.

2. No clear distinction between new and follow-up notifications

When responding to a data breach, organisations must rapidly establish the scope, impact, and root cause of the incident so that notification can be made within the legal deadline. In that context, a first notification will often necessarily be approximate or high-level, for example because not all relevant facts have yet been established with certainty. Article 33(4) GDPR expressly recognises this reality by allowing information to be provided in phases. Other Regulations such as the Cyber Resilience Act also allow the reporting to be tiered

with shorter deadline for initial and high-level notification and longer for the final report, reflecting the fact that information is likely to be scarce at early stages of an incident. Furthermore, the excessive length of the template could significantly increase the likelihood that controllers will need to send multiple follow-up notifications to clarify inaccuracies in the original notification and/or add information on a phased basis which was not previously available.

We recommend that the template make this distinction explicit, so that it is clear an initial notification is not expected to contain the same level of completeness as a subsequent, follow-up submission.

Furthermore, we also recommend taking the DPC's approach for follow-up / supplemental notifications as an example: The DPC has a short webform with a free text box that allows the controller to provide additional information to supplement their previous report. This is a much better position than having to complete the entire questionnaire again (potentially multiple times).

3. No Early Check on the Notification Threshold

Before asking for any details, the form should first establish whether the incident actually meets the bar for notifying supervisory authorities, that is, whether it poses a likely risk to affected individuals, per Article 33. Ireland's DPC already builds this check into its own form. Without a similar safeguard here, smaller organisations unfamiliar with when notification is legally required risk two outcomes: filing reports that were never necessary, or ploughing through most of the document only to discover (at question 89 of the template), that they didn't need to submit anything in the first place.

DOT Europe's Key Recommendations
Proportionality: Substantially reduce the number of fields to align with Article 33(3) GDPR's four core notification elements, benchmarking against existing national templates that are considerably shorter.
Phased notification: Expressly confirm, in line with Article 33(4) GDPR, that an initial notification may contain approximate or high-level information, with detail completed through a follow-up notification. Encourage the EDPB to follow the DPC approach for follow-up notification.
Protection of sensitive information: Ensure technical descriptions and attachments do not compel disclosure of cyber-sensitive data, trade secrets, or privileged material, with clear assurances on confidentiality where such disclosure is genuinely required.
Objective reference frameworks: Anchor severity and risk-assessment fields to an established methodology (e.g. the ENISA severity assessment framework) and clarify the expected depth of the risk-assessment methodology description.
Cross-border simplification: Consolidate the supervisory authority list into a single list including the lead authority, and limit location-related fields to jurisdictions actually affected by the breach.
Legislative alignment: Align the 72-hour logic and risk-threshold fields with the pending Digital Omnibus proposal, and design the template as a single instrument capable of satisfying both GDPR and ePrivacy notification obligations.

2. Identification of the Data Controller and the Reporting Person

Field 26 – Accuracy & Responsibility

Field 26, read alongside the heading of section 2.2 ("Identity of the reporting person") and its accompanying Article 13 reference, appears to place liability on the individual submitting the notification, rather than on the controller organisation itself. We do not see any grounding in the GDPR for attaching personal liability to the person completing the form on the organisation's behalf. Field 25 compounds this concern by requiring the reporting person to supply their national identification number, a requirement equally without statutory basis under the GDPR. Article 87 GDPR further allows Member States to impose additional conditions on the processing of national ID numbers, and in some Member States such processing is prohibited outright absent explicit authorisation under national law. We encourage the EDPB to:

(i) ensure that accountability remains correctly placed with the controller;

(ii) remove any requirement to provide national ID numbers ensuring consistency with national law requirements.

If the liability stays with the controller, it should be clarified that this liability cannot extend beyond what the controller could reasonably know at the time of notification. This is directly linked to our comment above on the need to distinguish between new and follow-up notifications: liability for accuracy should be assessed against the information reasonably available at each stage, not against a standard of completeness that the short notification window makes impossible to meet.

Field 41 – Contact details of the other involved party.

Field 41 requires the controller to provide contact details for processors and other involved third parties. We ask the EDPB to specify what type of contact information is expected to be provided. The current form creates ambiguity as to the level of detail that controllers are obliged to supply in this section. We also recommend taking the DPC's approach for this information in their data breach notification form where this information is optional

3. Initial Information on the Personal Data Breach

Field 49 – Reasons for Late Notification of the Personal Data Breach

Field 49 is triggered once the 72-hour period following awareness has elapsed. This logic is hard-coded into the template, yet the ongoing Digital Omnibus proposal may revise the underlying notification trigger itself (see further below). We recommend that the EDPB confirm this field's logic remains consistent with any amended trigger before the template is finalised, to avoid adopting a template that is already out of step with the legislative framework it implements.

Field 52 and 53 – Further Comments on timeline and Additional Information

Fields 52 and 53 require disclosure of the date on which the data processor became aware of the personal data breach. While Article 33(2) GDPR requires processors to notify controllers without undue delay, they do not require that a precise awareness date be documented or disclosed as part of the notification. We request that the EDPB clarify, in the accompanying guidance, that receipt of a third-party notification alone does not constitute "awareness" within the meaning of Article 33 GDPR for the purposes of triggering the 72-hour notification obligation. Requiring this level of detail risks transforming the notification process into an assessment of the processor's own compliance, which falls outside the scope of what Article 33 was designed to capture.

Field 57 – Was the data unintelligible to anyone not authorised to access it or were individuals not identifiable?

Field 57 asks the controller to assess whether affected data was unintelligible to unauthorised persons or whether individuals were not identifiable. If the data were truly unintelligible or if individuals were genuinely not identifiable, it is unclear how the breach would meet the reporting threshold triggering a notification

obligation. We encourage guidance on how this field should be interpreted and on what basis a controller is expected to assess "unintelligibility" or "non-identifiability" for a breach that has already met the reporting threshold, in particular in light of the draft Digital Omnibus Regulation notification threshold and the EDPB's forthcoming anonymisation and pseudonymisation guidelines.

Field 58 – Type of integrity breach.

Field 58 requires the controller to classify the type of integrity breach, including whether alteration occurred without evidence of illegal or wrong use, or with such evidence but with the possibility of reversing or recovering damages. The draft GDPR Omnibus Regulation proposes a revised threshold for the notification obligation to the supervisory authority. Where damages are absent or reversible, it is unclear how the breach would meet that proposed threshold, therefore, the rationale for requiring notification in such circumstances is unclear. We welcome clarification as to how these integrity-breach categories interact with the proposed threshold for notification in the draft GDPR Omnibus Regulation.

Field 59 – Type of availability breach.

Field 59 requires the controller to characterise the type of availability breach, including whether the loss of availability is temporary, permanent, or not yet determined. We welcome the inclusion of this distinction, as the duration and nature of an availability incident are relevant factors in assessing risk to data subjects' rights and freedoms and whether such incident is reportable. However, we ask the EDPB to ensure that the criteria that controllers should apply when assessing whether a loss of availability, particularly a temporary one, are fully in line with the notification threshold under Article 33 GDPR or the notification threshold as proposed by the draft GDPR Omnibus Regulation. This would also help ensure that the form's characterisation options are applied uniformly across controllers and sectors.

Field 63 – Description of Systems, Software, Services and Infrastructure Involved

Field 63 requires a detailed, semantically grouped description of the systems, software and infrastructure involved in the breach, including their location. This level of detail goes significantly beyond what is required under Article 33 GDPR, therefore we respectfully suggest for the EDPB to reconsider its scope in line with what is necessary, reasonable and proportionate to a data breach notification. Providing this level of detail within the 72h regulatory deadline can be highly burdensome, particularly for a globally distributed controller where a single breach may span replicated infrastructure across dozens of jurisdictions, and the template offers no guidance on how to scope the concept of "location" in such cases. In addition, some of this information, for example forensic reports, system architecture, or details drawn from ransomware or phishing material, may be cyber-sensitive or constitute a trade secret and requiring excessive technical detail could itself introduce an additional security risk. Where, exceptionally, such information is genuinely necessary and its disclosure is not disproportionate, supervisory authorities should provide clear assurances that sensitive details will be protected and that legal privilege will be respected.

Field 65 – Categories of concerned data subjects.

Field 65 requires the controller to categorise affected data subjects across a range of classifications including customers, employees, minors, patients, subscribers, users, and vulnerable individuals. Controllers may not collect or retain the information to determine whether affected individuals fall into these categories. It should be clarified that a "not determinable" response is acceptable.

Field 72 and 73 – Personal data records concerned by the breach.

Field 72 and 73 requires disclosure of the number of personal data records concerned by the breach, including whether numbers are exact, approximate, undetermined, or to be determined. The methodological guidance distinguishes between five types of data about 100 people and 100 types of data about five people equating to 500 records in both instances. The EDPB should clarify the scope of 'records' for the purposes of this field and how the metric for controllers to respond consistently.

Fields 75-76 – 3.5 Measures in place when personal data breach occurred

Fields 75-76 request extensive information regarding the security measures in place at the time of the breach, including controls such as MFA, encryption, backups and auditing practices. Where the incident occurred within a data processor's environment, these fields may effectively compel disclosure of the processor's underlying security architecture. This goes beyond what Article 33(3)(d) GDPR requires, which focuses on the measures taken or proposed to address and mitigate the breach, not a comprehensive inventory of pre-existing safeguards

4. Further Information on the Personal Data Breach

Field 87 – Severity of the Potential Impacts

Field 87 asks controllers to self-assess severity as minor, moderate, severe, or to be determined, but the template proposes no reference framework for making that assessment. Absent such a framework, self-assessments are likely to vary considerably between controllers, undermining the comparability the EDPB is seeking to achieve. It is also unclear whether this field is intended to capture a distinct assessment from the risk assessment required by Fields 89-90, or whether they overlap and should be consolidated. We recommend that Field 87 be accompanied by an appropriate methodology, such as the ENISA recommendations for assessing the severity of personal data breaches and request clarification on whether this field serves a separate purpose from the risk assessment or whether the assessment should me merged.

Field 89 – Outcome and Methodology of the Risk Assessment

We further encourage an explanation on the intended relationship between Fields 87 and 89, including whether one should inform the other.

The draft Digital Omnibus Regulation would raise the Article 33 GDPR notification trigger from “a risk” to “a high risk”. Several fields in Section 4, including Field 89's options, presuppose the current, lower threshold, which raises the question of why a controller would need to complete those fields for breaches that would no longer trigger notification under the amended standard. We recommend that the EDPB confirm how this pending change has been factored into the template, and revise or remove any fields that would become inconsistent with the amended threshold.

6. Cross-Border Processing and Related Issues

Field 110 – Has the incident been notified to other supervisory authorities or control bodies under other relevant legislation?

Field 110 asks whether the incident has been notified to other supervisory authorities or control bodies under other relevant legislation, citing national cyber security centres as an example. The form does not clarify which regulatory frameworks this field is intended to capture, for example, whether it extends to notifications under the EU AI Act, ePrivacy Directive national implementing authorities, NIS2 obligations, the incoming Cyber Resilience Act (“**CRA**”) or other sectoral regimes. It also fails to specify whether the question is limited to notifications already made or whether it also encompasses those planned or under assessment. Last but not least, it also remains unclear what the legal basis for this question is.

Field 111 – Further information about notification to other authorities or bodies.

Field 111 requires controllers to provide further information about notifications made to other authorities or bodies, including the authority name and, where possible, the case ID. It is unclear why a GDPR breach notification form requires disclosure of notifications made under separate regulatory regimes. The EDPB does not explain whether it is intended for coordination, to avoid duplicative investigations, or to assess the

broader regulatory landscape of the incident. It is also unclear whether controllers are expected to update this field retrospectively if parallel notifications under other regulatory obligations, such as NIS2, the CRA or the AI Act, are triggered after the GDPR notification has already been submitted, given that different frameworks operate on different notification timeframes. We encourage the EDPB to clarify (i) the purpose of requiring cross-regulatory notification details within a GDPR breach form and what the legal basis for this field is, and (ii) whether there is an expectation to update this field if parallel notifications under other regulatory obligations are triggered at a later stage.

Fields 115 and 118 – Establishments and Supervisory Authorities

We would query why Field 115 requires listing every EEA country where the controller has an establishment, irrespective of whether all those establishments are actually affected by the breach in question; this field should be limited to jurisdictions genuinely concerned by the incident. Similarly, Field 118's framing around "other" supervisory authorities is unclear: we recommend a single list of supervisory authorities that includes the authority to which the controller is reporting, rather than a separate category, so that the form can be completed once and submitted to each impacted Member State rather than needing to be reformatted for every jurisdiction.

Field 118 requires controllers to list the EEA supervisory authorities to which the breach has been or will be notified, but, similarly to Field 115, its framing around "other" supervisory authorities is unclear. In particular, the EDPB does not clarify how this field should be completed in practice under the One-Stop-Shop ("OSS") mechanism. It is unclear whether the controller is expected to list each concerned supervisory authority for every EEA country where affected data subjects reside, or only those authorities to which the controller is directly notifying (i.e., the lead supervisory authority, with cross-border dissemination handled by that authority).

We would welcome clarification from the EDPB as to (i) whether Field 118 is intended to capture only direct notifications by the controller or also onward notifications made by the lead authority under the OSS mechanism, and (ii) whether controllers should list each relevant country-level authority individually or only those to which they are directly reporting. We recommend a single list of supervisory authorities that includes the authority to which the controller is reporting, rather than a separate category, so that the form can be completed once and submitted to each impacted Member State rather than needing to be reformatted for every jurisdiction.

Scale-appropriate design for location and infrastructure disclosure

The template requires granular disclosure of systems, infrastructure and processing locations, but offers no guidance on how a globally distributed controller should scope the concept of "location", particularly where a single breach spans replicated infrastructure across dozens of jurisdictions. We recommend that the EDPB clarify the expected level of granularity and consider whether requiring this degree of technical detail is proportionate, or whether it could itself introduce an additional security risk.

7. Attachments

Field 125 – Identification of Attachments

As with Field 63, several of the attachment categories listed, including ransomware notes, phishing messages, and forensic research reports, may contain highly sensitive or cyber-sensitive material. We support this field remaining optional and recommend that accompanying guidance reaffirm that supervisory authorities will treat such attachments with the same degree of confidentiality protection sought in respect of Field 63.

Alignment with Other EU Legal Instruments

Digital Omnibus

As noted above, the pending Digital Omnibus proposal may directly affect the template's hard-coded 72-hour logic (Field 49) and its risk-based structure (Field 89). We recommend that the EDPB take account of this pending legislation and confirm that the template will be updated, as necessary, before final adoption, so that it does not need to be substantially reworked shortly after entering into use.

ePrivacy Directive

The template addresses only the Article 33 GDPR notification obligation, without acknowledging the parallel obligation under Article 4 of the ePrivacy Directive. This risks requiring organisations subject to both regimes to file duplicative notifications across divergent national transpositions. We recommend that the EDPB design the template as a single instrument capable of satisfying both the GDPR and ePrivacy Directive notification requirements, thereby reducing the burden of multi-regime, multi-jurisdictional reporting. The EDPB should also allow organisations to make further submissions on any updates to the guidelines once the Omnibus legislative process has concluded.

Geographical scope and relationship with national templates

It remains unclear how the proposed EDPB template will relate to existing national supervisory authority templates. Should national templates ultimately be replaced by a final EDPB template, nothing should prevent a single-submission approach, whereby one notification to the lead supervisory authority satisfies Article 33 GDPR in respect of all concerned authorities, rather than requiring separate submissions across Member States.

Conclusion

DOT Europe supports the EDPB's ambition of a harmonised, cross-EU approach to personal data breach notification. A genuinely proportionate common template can benefit data subjects and controllers alike, by improving legal certainty and the comparability of notifications received by supervisory authorities.

As currently drafted, however, the template's length, level of technical granularity, and lack of accommodation for the operational realities of fast-moving incident response risk undermining that objective, increasing the compliance burden without a corresponding improvement in data protection outcomes. Nor does the template, in its current form, appear future-proofed against the pending Digital Omnibus reforms or aligned with parallel ePrivacy obligations.

DOT Europe therefore calls on the EDPB to revise the template in line with the principles reflected throughout this response:

Summary of Key Asks
Proportionality: Cut the template down to a workable length consistent with Art. 33(3) GDPR; do not exceed what SMEs can realistically deliver within the notification deadline.
Flexibility: Make explicit that a first notification may be incomplete and approximate, per Art. 33(4), with a follow-up notification used to complete the record.
Confidentiality: Protect cyber-sensitive information, trade secrets, and privileged material in technical fields and attachments.
Consistency: Provide reference methodologies for severity and risk-assessment fields, and clarify the expected scope of the risk-assessment narrative.

Simplification: Streamline cross-border fields (establishments, affected countries, supervisory authorities) into a single-submission logic.

Future-proofing: Revisit the 72-hour and risk-threshold logic in light of the Digital Omnibus, and design the template to also satisfy ePrivacy Directive Article 4 obligations.

DOT Europe would welcome the opportunity to discuss these recommendations further with the EDPB and stands ready to contribute to a revised template that genuinely advances data protection outcomes across the EU.