PrivacyRules: global alliance of data protection and cybersecurity experts

Feedback to the European Data Protection Board template for personal data breach notification Version 1.0

With the expert contribution of:

Background

About PrivacyRules

PrivacyRules was formed in 2016 by a group of legal and tech experts across Europe and America (https://www.privacyrules.com/) to address the growing demand for data protection and cybersecurity services. Launched in 2018, PrivacyRules is the world's only leading professional alliance of data privacy experts from the legal, tech and crisis communication disciplines. We formed this alliance to provide integrated and effective assistance and services to multinational companies and institutions.

Since 2017, we have grown dramatically, now with members in jurisdictions across the world and a number of tech, cybersecurity, and public relations companies within the alliance or cooperating with us. With our members we offer unique services combining legal and technical advice to avail multinational clients of implementable, holistic data privacy solutions on all continents.

In addition to organising webinars, podcasts, in person conferences and e-conferences, PrivacyRules disseminates independent information on data privacy matters via all its platforms. In this way, our alliance contributes to the global awareness about privacy and is an active contributor to the international dialogue on data protection and cybersecurity. PrivacyRules is honoured of regularly meeting and discussing with institutional interlocutors at national and international level, including with the European Data Protection Board.

To find out more about us, please visit our website or LinkedIn.

About this document

PrivacyRules recognises the fundamental role of the European Data Protection Board (hereafter "EDPB") for the consistent application of data protection rules throughout the European Union (hereafter "EU"), for the cooperation between the EU's Data Protection Authorities, and for its relevance at international level since the EU data privacy interpretation and application has impact at global level.

In relation to the EDPB Template for personal data breach notification (hereafter "the Template"), our members are therefore pleased to provide the below feedback structured on the following high-level issues:

1. Brief description of the high-level issue of the Template commented on;
2. Feedback on the high-level aspects regarding legal, practical, technical, or usability issues that may arise when a controller uses this part of the Template to notify a personal data breach;
3. Proposed amendment, clarification, additional response option, or change to the Template's mandatory status or business logic.

We are therefore pleased to submit this feedback with the aim of bringing to the EDPB's attention comments on the Template from experienced EU legal practitioners.

Copyright PrivacyRules© - All rights reserved 2016-2026

Executive Summary, part 1

The main concerns raised by PrivacyRules members can be summarised as follows:

1.The initial notification is overly complex and burdensome

The proposed Template contains a very large number of fields and requires detailed legal, technical and organisational information that may not be available within the initial 72-hour period. The Template should therefore clearly distinguish mandatory, conditional and optional information, allow controllers to indicate that certain matters remain under investigation, and reserve more detailed questions for follow-up notifications.

2.The distinction between initial, incomplete and follow-up notifications requires clearer business logic

The Template does not sufficiently explain how initial, incomplete and follow-up notifications should differ in practice. Controllers should be able to submit limited information at the initial stage, update it progressively, correct or withdraw erroneous notifications, and use standard responses such as "under investigation" or "not yet determined" without being prevented from submitting the form.

3.Greater guidance is required on awareness and risk assessment

The Template should distinguish more clearly between technical detection of an incident and the moment when the controller becomes aware of a personal data breach for the purposes of the 72-hour deadline. It should also provide practical and consistent criteria for assessing risk and high risk, while ensuring that any automated or suggested classification remains subject to the controller's reasoned assessment.

4.The Template requests excessive or sensitive technical information

Some fields appear to require highly detailed information about IT systems, vulnerabilities, attack vectors, forensic findings and remediation measures, which may exceed Article 33(3) GDPR and expose sensitive security or commercially confidential information. Mandatory disclosures should be limited to what is necessary, with detailed technical information provided only upon specific request and through secure channels.

5.Attachments and communications to data subjects should be limited and proportionate

The attachment checklist should be clearly identified as optional and illustrative, since relevant documents may be unavailable within 72 hours, confidential, privileged or connected with an ongoing investigation. Similarly, controllers should generally be allowed to confirm compliance with Article 34 GDPR through a structured checklist rather than being required to submit complete copies of communications containing personal data.

6.Predefined categories and response options require clarification and expansion

Several predefined terms and categories are unclear, incomplete or not fully aligned with GDPR terminology. The Template should provide clearer definitions, broader and more flexible response options, and appropriate categories for complex or emerging incidents, including supply-chain breaches, AI-related incidents and situations where communication to data subjects is ongoing, planned or not required.

Copyright PrivacyRules© - All rights reserved 2016-2026

Executive Summary, part 2

7.Coordination in multi-party and cross-border cases remains unclear

Controllers may not be able to determine the competent supervisory authority, the cross-border nature of the incident or the allocation of responsibilities among joint controllers and processors within the initial reporting period. The Template should permit provisional assessments, facilitate coordination and transfer of notifications between authorities, and avoid duplicate reporting on the same incident.

8.The Template should be interoperable with other EU incident-reporting regimes

The same incident may trigger parallel reporting obligations under the GDPR, NIS2, DORA and other sector-specific regimes. To reduce duplication, the EDPB should coordinate with other relevant EU bodies, publish a structured and reusable data model, and ensure that the Template is available in an editable and commonly used format.

9.Harmonisation requires substantive guidance, not merely a common form

A common Template alone will not ensure consistent breach notification practices across Member States. It should be accompanied by practical guidance, examples and a harmonised methodology for determining whether notification is required and for evaluating the likelihood and severity of risks to affected individuals.

10.DPOs should remain authorised to submit breach notifications

Field 23 appropriately confirms that a data protection officer may submit a breach notification on behalf of the controller. Given that Polish supervisory authority has questioned this practice on conflict-of-interest grounds under Article 38(6) GDPR, the EDPB should expressly retain this option in the final version of the Template.

While these are the principal high-level concerns, PrivacyRules members have raised additional legal, technical and usability concerns, which the EDPB is encouraged to consider in full when finalising the Template. These concerns are detailed below.

This brief introduction of the given feedback has been developed by **Dominika Nowak-Byrtek,** Managing Associate at **Traple Konarski Podrecki & Partners**, the PrivacyRules exclusive member firm for Poland.



Dominika Nowak-Byrtek
Managing associate at
Traple Konarski Podrecki & Partners

Copyright PrivacyRules© - All rights reserved 2016-2026

PrivacyRules members' comments on the template for personal data breach notification

- Comments on version 1.0 of 8 June 2026

	Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Belgium Contribution from **Lotte de Graeve, Associate at** TIMELEX	General structure, lack of interoperability with parallel incident-notification regimes (notably NIS2 Article 23, and other sectoral regimes such as DORA), and Section 6.1 on notifications to other authorities	The template is built as a standalone GDPR-only form and does not map its fields to the substantively overlapping information required under NIS2 and other incident-reporting regimes. Controllers who qualify as NIS2 essential or important entities must therefore reconstruct largely the same factual record (timeline, systems/services affected, impact, mitigation measures) in a differently structured national CSIRT notification, within an equally tight deadline. This duplicative effort runs counter to the "single reporting" ambition underlying the Digital Omnibus.	Publish the template's underlying data model in a structured, interoperable format (e.g. a documented schema) and coordinate with ENISA/NIS2 Coordination Group on a field-level correspondence table between the Article 33 template and NIS2 Article 23 notifications, so a single incident record can be reused or pre-populated across regimes.

Copyright PrivacyRules© - All rights reserved 2016-2026

Bulgaria
Contribution from
Martin Zahariev, PhD - Partner;
Desislava Krasteva, CIPP/E, CIPM - Partner;
Nevena Dobreva - Associate at

DPC
Dimitrov, Petrov & Co.

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Field 14	Unclear distinction between public and private sector in the GDPR. Could create confusion for private entities that provide public services (e.g. electricity, heat, water supply, transport, etc.) in which category do they fall.	Consider removing field 14.
General structure – template length and complexity	The template as a whole is excessively long and burdensome for a notification that must be submitted within 72 hours (or 96 under the pending Omnibus proposal). Controllers have a really short time span to report a breach once they become aware of such and often before the facts are fully established. Requiring this volume of granular information at this initial stage is disproportionate and risks becoming an obstacle to timely reporting rather than a tool to facilitate it. A non-exhaustive list of examples of overcomplicated or too granular content exceeding the minimum content required as per Article 33 (3) GDPR and/or having the potential to create significant difficulties for all types of controllers (not only SMEs, but also larger organisations with more complicated internal processes and structures) include Fields 4, 5, 7, 15, 16, 17, 25, 33-36 which could be merged with the info about the reporting person, as it seems overly complicated to have different reporting person and contact point for additional information, 44-47 which could be merged in one field, 56-61, 66-68 which could be merged in one field, etc.	Substantially simplify the template by reducing the volume of fields required at the initial notification stage to those geniuenly necessary under Article 33(3) GDPR, (i) merging certain fields together (33-36 and info for reporting person), 44-47, 66-68 and (ii) removing certain fields which are not required as per the GDPR (4, 5, 7, 15, 16, 17, 56-61). Leverage the template's existing "Incomplete notification" mechanism more broadly and by default, instead of treating full completion as the norm at this stage.

Copyright PrivacyRules© - All rights reserved 2016-2026

Bulgaria
Contribution from
Martin Zahariev, PhD - Partner;
Desislava Krasteva, CIPP/E, CIPM - Partner;
Nevena Dobreva - Associate at

DPC
Dimitrov, Petrov & Co.

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
General structure - template format	In its current form the template appears to be operational as an online form where certain fields are visible/unlocked depending on previous choices and does not appear to be downloadable in a commonly used human readable and editable format (e.g. .doc, docx, .pdf, etc.). This is a genuine practical constraint for transnational breaches affecting international organisations who need to coordinate a single breach across multiple jurisdictions and where data must be shared among internal/external legal, privacy, security, and compliance teams in a consistent manner. Currently the whole responsibility for filling it falls on the reporting person, whereas often the finalising of the notification content is a result of multiple efforts of different teams, sometimes from different jurisdictions.	Publish the template, including all fields, response options, and business logic, in a commonly used human readable and editable format (e.g. .doc, docx, .pdf, etc.). This would improve consistency, remove duplicate efforts, and enable more efficient cross-border incident management.
Section 4.1. (Fields 79, 81, 83)	Predefined lists (Fields 79, 81, 83) may unintentionally constrain how controllers describe the actual consequences and impact breach or provide other information relevant for the breach. Given the evolving nature of technologies, threat actors, and attack methods, any static list risks becoming incomplete over time. Where free-text explanations are only available under an "other" option, controllers may feel encouraged to fit incidents into predefined categories rather than accurately describe them.	Restructure these fields so free-text description is available and equally prominent alongside the predefined options in all cases – not only when "other" is ticked. The predefined options should guide reporting, not limit it, ensuring supervisory authorities receive a complete and fact-specific description of the breach. In any case, providing free-text answers where possible should be encouraged.

Copyright PrivacyRules© - All rights reserved 2016-2026

Bulgaria
Contribution from
Martin Zahariev, PhD - Partner;
Desislava Krasteva, CIPP/E, CIPM - Partner;
Nevena Dobreva - Associate at

DPC
Dimitrov, Petrov & Co.

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Fields 26, 65, 70	Several fields use terminology that is either undefined, ambiguous, or not clearly linked to GDPR requirements. This creates legal uncertainty and may lead to inconsistent reporting between controllers. For example, Field 26 does not clearly explain what the reporting individual is certifying, particularly because at this stage many of the facts remain under investigation. In addition, often the information is collected from various teams and the reporting person is practically not able to check and verify everything notified to the data protection authority. The ultimate responsibility is in any case for the data controller and this field creates confusion and misunderstanding. Field 65's closed list of data subject categories is not precise, the suggested options appear to be restrictive and confusing, in particular where patients, minors, students are listed as not "vulnerable" individuals even though they may be (e.g. GDPR, in Recital 75, recognises children as a particularly vulnerable group). While some of the categories are objective (e.g. customers, employees, etc.), the notion of "vulnerability" is contextual and depends on the specific facts of the case. The GDPR does not contain a clear definition of the term "vulnerable" either and does not contain specific rules for the processing of personal data of vulnerable persons - it is used only in the context of risk assessment. Other often affected categories (job candidates, former employees, etc.) are missing. "Official documents" as referenced in Field 70 lacks sufficient description as to whether these are identity documents or encompass some other categories of official documents (administrative acts, certifications, diplomas, etc.).	Align terminology more closely with GDPR concepts and either define ambiguous terms or remove them. Refine the categories of affected subjects and remove "vulnerable" as a notion. Where categories are retained, accompanying guidance should explain their meaning and purpose to ensure consistent interpretation across Member States.

Copyright PrivacyRules© - All rights reserved 2016-2026

Bulgaria

Contribution from
Martin Zahariev, PhD - Partner;
Desislava Krasteva, CIPP/E, CIPM - Partner;
Nevena Dobreva - Associate at

DPC
Dimitrov, Petrov & Co.

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 7 (Attachments)	The attachment checklist includes documents that controllers do not have an explicit legal obligation to maintain or possess (e.g. copy of the internal procedure to notify a data breach) or documents that may be needed by the law enforcement authorities for pending criminal investigation (ransomware or phishing related communications) and therefore cannot be disclosed at this stage. This may create the impression that such documents are expected in every case, generating unnecessary follow-up queries or assumptions of non-compliance where a document simply does not exist or cannot by provided by virtue of a law enforcement authority prescription. In some instances, even if such documents exist, they may be maintained in English or other foreign language which is the working language of an international group of companies and therefore these cannot be objectively provided in the official language of the proceedings within 72 hours with the first notification. That is why it is preferrable to receive concrete follow-up requests for these documents by the data protection authority at a later stage.	Clarify in the field's tooltip that the attachment list is illustrative and optional, applicable only where such a document happens to exist and the controller is able to provide it within the 72-hour period, and that the absence or non-provision of any listed document is not itself indicative of non-compliance or an incomplete notification. Include an indication if there is a requirement for translation in local language of attachments and provide explanation that in such cases translated documents may be provided at a later stage.

Copyright PrivacyRules© - All rights reserved 2016-2026

France

Contribution from **Jean-Christophe Chevallier, Partner at** VDÈS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 1.1, "Type of notification", in particular the predefined options "Complete" and "Incomplete", and the business logic applicable to mandatory fields.	When an initial notification is made within the 72-hour period, the controller will frequently be unable to provide reliable information regarding the scope, root cause, duration or consequences of the breach. If all mandatory fields require a substantive answer even for an "Incomplete" notification, the controller may be compelled either to provide speculative information or to delay the notification.	For an "Incomplete" notification, allow the controller to select"Under investigation", "Not yet determined" or "Estimate unavailable at this stage" for any information that is not yet available. The business logic should permit submission of the initial notification once the minimum information reasonably available to the controller has been provided.
Section 3.1, "Date and time of the personal data breach and of its detection".	The date on which a security incident is technically detected does not necessarily correspond to the date on which the controller becomes "aware" that a personal data breach has occurred within the meaning of Article 33 GDPR. At the time of the initial alert, the controller may not yet have a reasonable degree of certainty that personal data have been compromised. Conversely, the exact start or end date of the breach may remain unknown after the controller has become aware of it.	Add three separate fields for:(i) the known or estimated start and end dates of the breach;(ii) the date and time on which the security incident was first detected; and(iii) the date and time on which the controller became aware that a personal data breach had occurred. The tooltip should clarify that the 72-hour period is assessed by reference to the awareness date. Estimated dates or date ranges should be permitted.
Sections 3.2 to 4.4, in particular the mandatory status of fields relating to the circumstances of the breach, security measures in place, likely consequences, mitigation measures and measures intended to prevent recurrence.	Some of the requested information appears to go beyond the minimum information required under Article 33(3) GDPR. It may also be unavailable during the initial 72-hour period. Requiring detailed information on the root cause, existing security arrangements or measures intended to prevent recurrence may delay notification and create uncertainty as to whether optional contextual information has become mandatory in practice.	Clearly distinguish between:(i) information required under Article 33(3) GDPR;(ii) information required only where relevant and available; and(iii) optional contextual information. Fields falling within categories (ii) and (iii) should not prevent submission of an initial incomplete notification and should be capable of being completed through a follow-up notification.

Copyright PrivacyRules© - All rights reserved 2016-2026

France

Contribution from
Jean-Christophe Chevallier, Partner at
VDÈS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 4.2, "Assessment of the risk to the rights and freedoms of natural persons", including any predefined risk level, response option, scoring mechanism or related tooltip.	A predefined risk level or automated scoring mechanism may oversimplify the assessment by relying primarily on the categories or volume of data concerned. The actual risk is contextual and also depends on factors such as the vulnerability of the individuals, ease of identification, duration of exposure, identity of the unauthorised recipient, likelihood of misuse and effectiveness of encryption or other safeguards. There is also a risk of confusion between the "risk" threshold under Article 33 and the "high risk" threshold under Article 34 GDPR.	Clarify that any predefined level or scoring result is indicative only and does not replace the controller's contextual assessment. Allow the controller to override the suggested level and explain its assessment in a free-text field. The tooltip should clearly distinguish between"risk" under Article 33 GDPR and"high risk" under Article 34 GDPR, and provide a concise, non-exhaustive list of relevant assessment factors.
Section 5, "Communication to the data subjects", including the predefined response options and conditional mandatory fields.	A simple "Yes/No" response does not reflect all situations contemplated by Article 34 GDPR. Communication may be ongoing, planned or carried out in stages. It may also be unnecessary because no high risk was identified or because one of the exceptions under Article 34(3) applies. A negative response may therefore be incorrectly understood as indicating non-compliance.	Add the following predefined options:(i) communication completed;(ii) communication ongoing;(iii) communication planned;(iv) communication not required because no high risk was identified;(v) communication not required under Article 34(3)(a);(vi) communication not required under Article 34(3)(b); and(vii) public communication or similar measure used under Article 34(3)(c). A free-text field should allow the controller to explain its assessment.
Section 6.1, "Whether other authorities or bodies have been notified", including the mandatory status of the related fields.	A personal data breach may trigger parallel obligations under cybersecurity, financial, healthcare, telecommunications, criminal or insurance rules. The relevant authorities and applicable reporting requirements vary significantly between Member States and sectors. During the initial 72-hour period, the controller may not yet have completed its assessment of all parallel obligations. This information is not part of the minimum content expressly required by Article 33(3) GDPR.	Make this section optional and limited to notifications already made or clearly planned. Include non-exhaustive options for cybersecurity authorities, law-enforcement authorities, sectoral regulators, insurers and "Other". The tooltip should clarify that the information is collected for coordination purposes only and does not constitute an assessment of compliance with other legal instruments.

Copyright PrivacyRules© - All rights reserved 2016-2026

France

Contribution from **Jean-Christophe Chevallier, Partner at** VDÈS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 6.2, "Whether the personal data breach involves a cross-border processing", including the identification of the lead and concerned supervisory authorities.	During the initial 72-hour period, a controller may be unable to determine definitively whether the breach concerns cross-border processing or which supervisory authority is competent. The analysis may involve multiple establishments, systems, processors or categories of data subjects. Requiring a definitive answer may result in incorrect notifications or precautionary duplicate notifications to several authorities.	Add the response options"Provisional assessment" and"Under review". Allow the controller to identify its proposed lead supervisory authority and briefly explain the basis for that assessment, without treating the selection as definitive. The business logic should allow the competent authorities to transfer or share the notification without requiring the controller to submit a new notification.
Section 7, "Attachments", and all free-text fields requesting detailed information on vulnerabilities, attack vectors, security measures, forensic investigations or remediation.	Detailed technical information may itself be highly security-sensitive and could expose unresolved vulnerabilities, facilitate further attacks, compromise an ongoing investigation or affect third parties. Attachments may also contain unnecessary personal data, confidential information or material protected by legal professional privilege or professional secrecy. Controllers should not be encouraged to upload complete forensic or legal reports when a factual summary is sufficient.	Add a warning not to include passwords, credentials, exploitable technical details, unnecessary personal data or legally privileged documents. Allow information and attachments to be marked as"Confidential" or"Security-sensitive". Clarify that controllers may submit concise summaries or redacted documents and that additional sensitive information may be provided through a dedicated secure channel if strictly necessary.

Copyright PrivacyRules© - All rights reserved 2016-2026

Germany

Contribution from
Volker Wodianka, CEO at

Wodianka privacy legal

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 1.1, "Type/Sub-type of notification", Under the current business logic, the "Withdraw" sub-type option is only visible/selectable when "Type of notification" = "Follow-up Notification."	This leaves no way to withdraw a notification that was originally submitted as a new notification, for example a duplicate submission, or a case reported prematurely that turns outmnot to be a reportable breach at all.	Extend the visibility condition so that "Withdraw" is also selectable when "Type of notification" = "New Notification," allowing controllers to retract a wrong first-time submission through the same mechanism.
Section 3.2, "Description of the systems, software, services and infrastructures", the field asks controllers to list, in detail, the systems, databases, software and their physical/logical location	This level of granularity effectively requires disclosing internal IT architecture and indirectly the attack surface of the organisation. Article 33 (3) GDPR does not require this degree of technical detail, and producing it may constitute a disproportionate effort especially for SMEs without a clear corresponding benefit for the authority's risk assessment. It also creates a security concern: detailed infrastructure descriptions mentioned in breach files can already be a sensitive asset.	Limit the mandatory response to the type of system or processing affected (e.g. "customer database," "HR system," "payment processing"), and make granular technical detail (server names, hosting location, specific software versions) only available to the authority if specifically requested during the follow-up communication and if genuinely needed for the specific case.
Section 4.1, "Severity of the potential impacts", the field only offers three severity levels: minor, moderate, severe, plus "to be determined," with no accompanying definition or assessment methodology in the tooltip.	Without objective, shared criteria, this rating is left almost entirely to the controller's own judgment. That undermines consistency across controllers reporting comparable incidents. The same underlying breach could plausibly be labelled "moderate" by one controller and "severe" by another.	Add methodological guidance to the tooltip, e.g. a short EDPB-defined set of criteria (e.g. number of affected data subjects, scale, special category data involved), so controllers apply a comparable standard rather than a purely subjective label.

Copyright PrivacyRules© - All rights reserved 2016-2026

Hungary

Contribution from **Endre Varady, Partner at**

VJT & PARTNERS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Overall template design and structure	The proposed template represents an important step towards harmonised personal data breach notification across the EU. However, incident reporting obligations under EU law are increasingly interconnected. A single cyber incident may simultaneously trigger notification obligations under the GDPR and other EU legislative frameworks (e.g. NIS2 or sector-specific cybersecurity legislation), while the underlying factual information required by the competent authorities is often substantially the same. As the template is intended to serve as a common EU notification framework, consideration should also be given to its longer-term interoperability with other incident reporting regimes. Without such consideration, there is a risk that future regulatory developments may require substantial redesign of the template or oblige organisations to maintain multiple reporting structures for the same incident, increasing administrative burden without improving regulatory oversight.	When finalising the template, the EDPB should consider adopting a structure and terminology that facilitate future interoperability with other EU incident reporting frameworks. While the template should remain focused on Article 33 GDPR, designing it with future convergence in mind could reduce unnecessary duplication, minimise future redesign efforts, and support the broader EU objective of coherent and efficient digital reporting obligations.
Risk assessment section (Fields 87–90) and the accompanying tooltips throughout the template.	The template contains numerous helpful tooltips and practical explanations that assist controllers in completing factual sections of the notification. For example, the template provides illustrative guidance on describing affected systems, estimating the number of records, etc. However, considerably less guidance is provided for those parts of the template that require controllers to exercise professional judgement. In particular, the template requires controllers to classify the severity of potential impacts (Field 87), determine whether the breach is likely to result in a risk or a high risk to the rights and freedoms of natural persons (Field 89), and describe the methodology used for their risk assessment (Field 90), without providing practical assessment criteria or examples.	The EDPB may wish to complement the risk assessment section with additional practical guidance, either through enhanced tooltips or an accompanying implementation guide. Such guidance could include illustrative assessment criteria, practical examples and recommended factors to consider when assessing the severity of impacts and distinguishing between different levels of risk. This would promote greater consistency in the application of the template while preserving the flexibility necessary for case-by-case assessments.

Copyright PrivacyRules© - All rights reserved 2016-2026

Hungary

Contribution from **Endre Varady, Partner at**

VJT & PARTNERS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
	As a result, controllers may apply different methodologies and thresholds to similar incidents, reducing the consistency and comparability of notifications submitted across the EU.	
Overall template structure and business logic governing initial and follow-up notifications.	The proposed template is comprehensive and represents a significant step towards harmonised personal data breach notification across the EU. The level of detail requested is generally appropriate and may contribute to more structured breach documentation and improved incident management. However, the overall template comprises approximately 126 fields, many of which are mandatory, while only a limited number are explicitly subject to conditional visibility rules. Although the template accommodates incomplete notifications through various response options (e.g. "to be determined", "under assessment"), the current specification does not clearly demonstrate how the overall reporting burden is reduced during the initial 72-hour notification. Consequently, controllers—particularly SMEs and organisations without dedicated incident response teams—may perceive the initial notification process as unnecessarily complex and time-consuming.	The EDPB may wish to review whether additional business logic could further streamline the initial notification stage by postponing certain detailed questions until follow-up notifications where appropriate. Alternatively, the consultation package could include an illustrative example (or screenshots) showing the practical workflow of an initial notification compared with a complete notification. This would enable stakeholders to better understand the intended operation of the phased notification mechanism and assess whether the reporting burden for the initial notification is proportionate.

Copyright PrivacyRules© - All rights reserved 2016-2026

Hungary

Contribution from **Endre Varady, Partner at**

VJT & PARTNERS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Overall objective of the common EU personal data breach notification template	The introduction of a common EU notification template is a significant step towards harmonising personal data breach reporting across Member States. However, harmonisation of the notification format alone may not result in fully harmonised notification practices. The decision whether a personal data breach is notifiable under Article 33 GDPR depends on the controller's assessment of the likelihood and severity of the risk to the rights and freedoms of natural persons. In practice, supervisory authorities and controllers may apply different methodologies or thresholds when carrying out this assessment. As a result, similar incidents may still lead to different notification outcomes across Member States despite the use of a common notification template.	The EDPB may wish to complement the template with additional guidance promoting a more consistent methodology for assessing the notification threshold under Article 33 GDPR, particularly regarding the assessment of likelihood and severity of risks. Greater convergence in these substantive assessments would further enhance the harmonising effect of the common notification template.

Copyright PrivacyRules© - All rights reserved 2016-2026

Poland

Contribution from
Dominika Nowak-Byrtek,
Managing Associate at

Traple Konarski Podrecki & Wspólnicy
TKP

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
2.2. Identity of the reporting person	Field 23 of the Form indicates that the person notifying a personal data breach on behalf of the controller may be the data protection officer within the meaning of Article 37 GDPR. From the Polish perspective, the European Data Protection Board's confirmation that a breach notification may be submitted by the DPO is highly significant, as the President of the Polish Personal Data Protection Office has previously questioned whether DPOs may perform such actions due to a potential conflict of interest within the meaning of Article 38(6) GDPR.	The EDPB should retain the option for DPOs to submit breach notifications in the final version of the Template.

Portugal

Contribution from
Helena Tapp Barroso
Partner
and
Adriana Alves Henriques
Associate Lawyer
at

ML MORAIS LEITÃO GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Fields 24 (Description of the function of the reporting person) and 25 (National Identification Number)	Since the reporting person's role is already indicated in Field 23, even where the "Authorised representative or other" option is selected, the identification number of the person and the description of the role may be considered not relevant for notification purposes.	Fields 24 and 25 should be of an optional nature.
Field 49 (Reasons for late notification of the personal data breach) and its tooltip	The field requests reasons for late notification but provides no guidance. Without guidance, controllers may provide legally insufficient reasons.	The tooltip for field 49 should provide examples of accepted justifications for delay (e.g. ongoing forensic investigation, inability to establish the extent of the breach within 72 hours, etc.).
Field 58 (Type of integrity breach) and its response options	In the case of some integrity breaches the controller may genuinely be unable to determine, during the initial phase of the investigation, whether any data was modified, whether such modification was malicious or accidental, and whether it is reversible. Contrary to what happens with other type of breaches, the template does not provide a option for "Not determined" or "To be determined".	Considering that it is a mandatory field, a "To be determined" option should therefore be included in line with other breach-type fields.

Copyright PrivacyRules© - All rights reserved 2016-2026

Portugal
Contribution from
Helena Tapp Barroso
Partner
and
Adriana Alves Henriques
Associate Lawyer
at

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Fields 62 (Further description of the nature of the incident), 63 (Description of the systems, software, services, and infrastructures involved in the personal data breach and where they are located), 66 (Further description of categories of concerned data subjects and additional data subjects), 71 (Further description of breached data and additional data categories), 76 (Further description of relevant measures in place when the personal data breach occurred) and their mandatory nature	These fields are designated as mandatory. However, many of them are additional-information fields whose subject matter is already captured in other fields of the template. Requiring detailed information in these fields on a mandatory basis may create uncertainty as to what is actually required under Article 33(3) GDPR and may delay notification.	The information legally required under Article 33(3) GDPR shall remain captured in the existing fields. The additional-information fields (save for those that should be used when the "Other" option is selected) should be of a non-mandatory nature.
Field 97 (Has the personal data breach been communicated to data subjects?) and its response options	The response options do not reflect all situations contemplated by Article 34 GDPR and also are not very clear from a user point of view.	The response options for field 97 should be revised as follows: option a) should be retained but clarified to refer to communication to all affected data subjects; a new option b) should be introduced to cover the situation where communication is ongoing but has not yet reached all data subjects, which avoids the controller inaccurately selecting "Yes" when the process is incomplete; this renders the corrective function of field 102 less necessary; options b) and b1) of the current template should be renumbered as c) and d) respectively, with d) restricted to incomplete notifications; option c) should be replaced by language that expressly references the risk assessment rather than the investigation, and should indicate on the face of the option that it is available only for incomplete notifications (renumbered as option e); option d) (current) should be retained (renumbered as option f); and option e) should be split into three separate options corresponding to each of the exceptions under Article 34(3) GDPR.

Copyright PrivacyRules© - All rights reserved 2016-2026

Portugal
Contribution from
Helena Tapp Barroso
Partner
and
Adriana Alves Henriques
Associate Lawyer
at
MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Fields 109 (Has the incident been reported to the police/judicial authorities as a criminal offence?), 110 (Has the incident been notified to other supervisory authorities or control bodies under other relevant legislation?), 113 (Does the personal data breach involve cross-border processing carried out by a controller established in the European Economic Area?), 114 (The lead supervisory authority is:) and 120 (Does the personal data breach involve processing, to which the GDPR applies, carried out by a controller that is not established in the European Economic Area?) and their response options	The use of the expression "Unknown" may suggest a static absence of knowledge, that the relevant information is simply not held, and may be read by the supervisory authority as a lack of diligence.	"Unknown" should be replaced by "To be determined / to be assessed"."To be determined / to be assessed", by contrast, conveys that the matter is actively under investigation and that a definitive answer is expected to follow, which accurately reflects the reality of the early phase of most breach responses.
General note: template design	A personal data breach may trigger parallel notification obligations under other applicable regimes (e.g. NIS2, DORA, or sector-specific cybersecurity legislation). This template has been designed only for GDPR compliance purposes, which may create duplication of effort for organisations who are obliged to do other notifications for the same incident.	The form should be designed to align with the parallel regimes: capturing, at the point of detection, the superset of fields all applicable notifications require, so a single intake feeds each output rather than forcing a full re-triage per regime. At minimum, the form should be structured so its GDPR fields map cleanly onto and are consistent with the corresponding NIS2/DORA fields, avoiding divergent factual accounts of the same incident across regulators.

Copyright PrivacyRules© - All rights reserved 2016-2026

Sweden
Contribution from
Helena Rönqvist, Partner
and
Marie Segerholm Associate
at
MAGNUSSON

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 2.2 (Field 25): National identification number of the reporting person – unnecessary and disproportionate data collection	Field 25 requests the national identification number of the reporting person. Collecting the national identification number of the DPO or other reporting person is unnecessary for the purposes of a data breach notification: the reporting person is already identified by name, function, and contact details (Fields 21–24). Requiring or even enabling the collection of a national identification number in this context risks constituting an unnecessary and potentially unlawful processing of the reporting person's own personal data.	Remove Field 25 (National identification number) from the template entirely, or at a minimum ensure that it is not implemented by supervisory authorities unless explicitly required by national law for identity verification purposes. The EDPB should consider whether collecting a national identification number from the reporting person is proportionate and necessary at all, given that identity can be established through other means already present in the form.
Section 2.4 (Fields 38–41): Involvement of other parties (joint controllers) – unclear allocation of notification responsibility	The template asks whether other parties are involved and requests their name and contact details, but does not include a field to record whether a joint controller has made a separate notification to its own supervisory authority. This creates a risk of duplicate notifications and coordination failures in multi-processor or multi-controller breach scenarios.	Add a field specifying whether a joint controller has filed a separate notification. The tooltip should clarify who bears the notification obligation vis-à-vis the supervisory authority in a joint-controller arrangement.
Section 3.2 (Field 60): Nature of the incident – absence of AI-related incident types and supply chain attacks	The predefined list of incident types is extensive but does not include: (a) AI model compromise or training data breach; and (b) supply chain attack (via third-party software or hardware). These are now more common. Directing controllers to the catch-all 'Other' option deprives supervisory authorities of structured, comparable data on these systemically significant breach types.	Add separate options for: (i) AI system or training data compromise; and (ii) supply chain attack (software or hardware from a third-party vendor).

Copyright PrivacyRules© - All rights reserved 2016-2026

Sweden

Contribution from
Helena Rönqvist, Partner
and
Marie Segerholm Associate
at

MAGNUSSON

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
Section 3.3 (Fields 65–68): Categories of data subjects – insufficient differentiation of children as a data subject category	The template lists 'Minors' as a single category of data subject, without distinguishing between children under 13 years of age and adolescents aged 13–17. This distinction is legally relevant: children under 13 cannot provide a legally valid consent in most Member States under Article 8 GDPR, and Recital 75 and Article 9 require a heightened risk assessment when their data is involved. The template does not prompt the controller to apply the enhanced level of protection required for this sub-group.	Split the 'Minors' category into: (i) children under 13 years of age, and (ii) adolescents aged 13–17. Add a tooltip noting the enhanced protection requirements. The risk assessment section (Field 89) should contain a corresponding reminder when this sub-category is selected.
Section 5 (Field 106): Content of the communication to data subjects – no minimum content checklist aligned with Article 34(2) GDPR	Field 106 requests the content of the communication sent to data subjects. However, such communications will frequently contain sensitive personal data relating to the affected individuals, or the specific nature of the breach as it affects them personally. Requiring controllers to submit this content in full to the supervisory authority creates an additional and unnecessary data flow involving the personal data of the very individuals the notification is intended to protect. Furthermore, the template does not specify the minimum content required under Article 34(2) GDPR, leaving controllers without clear guidance on whether their communication meets the statutory threshold.	Replace the requirement reproduce the full content of the communication with a structured checklist confirming that the information required under Article 34(2) GDPR has been provided to data subjects. If the supervisory authority requires access to the actual communication, this should be requested separately on a case-by-case basis through a dedicated secure channel, rather than collected as a matter of course from all notifying controllers.

Copyright PrivacyRules© - All rights reserved 2016-2026

Sweden

Contribution from
Helena Rönqvist, Partner
and
Marie Segerholm Associate
at

MAGNUSSON

Which section, field, predefined response option, tooltip, mandatory requirement, or business-logic rule of the personal data breach notification template does your comment concern?	What legal, practical, technical, or usability issue may arise when a controller uses this part of the template to notify a personal data breach?	What specific amendment, clarification, additional response option, or change to the template's mandatory status or business logic do you propose?
General structure – confidentiality of information submitted in the notification form	In Sweden, documents submitted to a public authority, including the Swedish supervisory authority (IMY), are in principle public records subject to the principle of public access to official documents (Sw. offentlighetsprincipen) under the Freedom of the Press Act and the Public Access to Information and Secrecy Act (OSL). A controller submitting a breach notification may therefore be unaware that detailed technical, commercial or operationally sensitive information included in the form – such as descriptions of IT infrastructure, security vulnerabilities, or internal investigation findings – could become accessible to third parties upon request. The template provides no guidance on this risk, nor any mechanism for the controller to flag information as sensitive or to request confidential treatment.	Add a prominent notice in the form explaining that information submitted to supervisory authorities may be subject to national rules on public access to official documents and may therefore be accessible to third parties. Encourage controllers to limit their submissions to information strictly necessary for the notification and to avoid including operationally sensitive details that go beyond what is required. Where a controller considers that specific information is commercially sensitive or operationally confidential, the form should allow that information to be flagged.
General structure – template length and complexity disproportionate for small and medium-sized organisations	The template comprises 126 fields across seven sections and requires a level of technical, legal and organisational detail that may be disproportionate for small and medium-sized enterprises (SMEs) and micro-enterprises. These organisations typically lack dedicated data protection teams, legal counsel or IT security resources. When confronted with a complex multi-page notification form during the acute phase of a breach – which must be submitted within 72 hours – smaller controllers may either delay notification, submit incomplete or inaccurate information under pressure, or incur disproportionate costs in seeking external assistance. The current structure does not adequately reflect the principle of proportionality.	Consider introducing a two-tier notification model. For the initial notification submitted within the 72-hour window, require only the minimum information mandated by Article 33(3) GDPR. All remaining fields should be reserved for follow-up notifications submitted once the controller has had a reasonable opportunity to investigate. This would make the template accessible to a broader range of controllers without reducing the quality of information available to supervisory authorities in the longer term.

Copyright PrivacyRules© - All rights reserved 2016-2026

On behalf of PrivacyRules, we would like to express appreciation for the EDPB's openness to receiving feedback about its Template from data privacy practitioners. We stand ready to provide additional clarifications regarding our comments, if and as needed.

PrivacyRules and its members contributing to this feedback authorise the publication of the present document and of the content of the feedback provided therein, in full or in part, wishing that the authorship of these comments will be credited.

Contributing PrivacyRules member firms

BELGIUM : TIMELEX ATTORNEYS	**GEERT SOMERS:** GEERT.SOMERS@TIMELEX.EU	TIMELEX
BULGARIA : DIMITROV PETROV & CO	**MARTIN ZAHARIEV:** MARTIN.ZAHARIEV@DPC.BG	DPC Dimitrov, Petrov & Co.
FRANCE : YDÈS	**JEAN-CHRISTOPHE CHEVALLIER** JC.CHEVALLIER@YDES.COM	YDÈS
GERMANY : WODIANKA PRIVACY LEGAL GMBH	**VOLKER WODIANKA** VOLKER.WODIANKA@PRIVACY-LEGAL.DE	Wodianka privacy legal
HUNGARY : VJT PARTNERS	**ENDRE VÁRADY** VARADY@VJT-PARTNERS.COM	VJT & PARTNERS

Copyright PrivacyRules© - All rights reserved 2016-2026

Contributing PrivacyRules member firms

POLAND : TRAPLE KONARSKI PODRECKI I WSPÓLNICY	**AGNIESZKA WACHOWSKA:** AGNIESZKA.WACHOWSKA@TRAPLE.PL	TKP Traple Konarski Podrecki & Wspólnicy
PORTUGAL : MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS	**HELENA TAPP BARROSO** HTB@MLGTS.PT	ML MORAIS LEITÃO GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS
SWEDEN : MAGNUSSON	**HELENA RÖNQVIST** HELENA.RONQVIST@MAGNUSSONLAW.COM	MAGNUSSON

Copyright PrivacyRules© - All rights reserved 2016-2026



CONTACT US

PrivacyRules

Global Headquarters:
PrivacyRules Ltd.
201 East Fifth Street
Suite 1900 – #1362
Cincinnati, OH 45202, USA

Email
info@privacyrules.com

www.privacyrules.com

Copyright PrivacyRules© - All rights reserved 2016-2026