EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Comments on the

European data Protection Board's Data Breach Notification Template

European Federation of Data Protection Officers

August 2026

The EFDPO Association welcomes the European Data Protection Board's initiative to develop a common template for personal data breach notifications. The objective of structuring, harmonizing, and unifying notification processes across the European Economic Area is important and timely. A common template can reduce fragmentation among supervisory authorities, support more consistent compliance with Articles 33 and 34 GDPR, and assist controllers, processors, Data Protection Officers, and supervisory authorities in handling breach notifications more efficiently. The EDPB has indicated that the template is intended to help organizations and DPAs structure, harmonize, and unify breach notification processes, and that it should help ensure notifications contain the information required by Article 33 GDPR .

We support the template's overall direction, including its use of structured fields, predefined options, and conditional logic. We also welcome the recognition that organizations may submit incomplete notifications and later supplement them. This is consistent with the practical reality that, in many incidents, the controller must notify within 72 hours while technical investigations, forensic analysis, and risk assessment are still ongoing. The GDPR requires notification to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons . The template's distinction between complete, incomplete, follow-up, and withdrawal notifications is therefore useful.

At the same time, we respectfully submit that several aspects of the template should be clarified or adjusted before finalization, in order to ensure that it remains proportionate, workable for organizations of different sizes and sectors, and legally aligned with the GDPR's risk-based approach.

General Comments

The template is extensive and, in several places, appears to request information that may be useful to supervisory authorities but is not always necessary for the initial notification required under Article 33 GDPR, which requires the notification to describe the nature of the personal data breach, including where possible the categories and approximate number of data subjects and records concerned. Also to communicate the name and contact details of the DPO or other contact points, describe the likely consequences and describe the measures taken or proposed to address the breach. The template should make clearer which fields reflect these legal minimum requirements and which fields are optional, recommended, or requested for supervisory authority triage.

This distinction is particularly important because the template may become the practical interface through which data controllers understand their legal obligations. If extensive operational, technical, sectoral, or organizational information is marked as mandatory, controllers may reasonably perceive that information as a legal prerequisite to notification. That could create friction with timely reporting, particularly during the first 72 hours of an incident.

We therefore recommend that the final template adopts a layered structure. The first layer should contain only the minimum information necessary to satisfy Article 33 GDPR and enables supervisory authority triage. A second layer should invite additional information where available. A third layer should support follow-up updates as the investigation progresses. This would preserve the template's usefulness while reducing the risk that controllers delay notifications while attempting to complete fields that are not yet known.

More particularly:

1. Mandatory Fields Should Be Narrowed for Initial Notifications

The template contains many fields marked as mandatory or conditionally mandatory, including fields relating to organizational identifiers, reporting person details, national identification number where applicable, detailed system descriptions, measures in place, country-by-country numbers, lists of other authorities, and attachment categories. Some of these fields may be useful, but not all will be available or necessary at the time of an initial notification.

We recommend that the EDPB distinguish more clearly between fields that are mandatory for all notifications, fields that are mandatory only for complete notifications, and fields that are optional or recommended for incomplete notifications. Where the template uses the option "to be determined" or "not yet known," that approach should be available consistently for all fields that may reasonably be unavailable during the first phase of an incident.

In particular, the fields concerning detailed descriptions of systems, software, services, infrastructure, and location may be difficult to complete accurately at an early stage. They may also raise security concerns if the submitted information is highly granular. We recommend that the template permit a high-level description at the initial notification stage, with more detailed technical information to be provided in follow-up notifications where necessary and proportionate.

2. The Template Should Better Reflect the Role of the DPO

The template properly includes fields for the name and contact details of the DPO or other contact point. However, the sections on the identity of the reporting person and the DPO should avoid creating the impression that the DPO is personally responsible for the accuracy of the notification or for the controller's breach response. Under the GDPR, the controller is responsible for compliance and for notifying the supervisory authority, while the DPO informs, advises, and monitors compliance.

We recommend that the template include a clear note that the DPO may be identified as a contact point without assuming personal responsibility for the facts, legal assessment, or operational decisions described in the notification. This clarification is particularly important for DPO independence and to avoid conflicts with the DPO's advisory and monitoring role.

The field titled “Accuracy & Responsibility” should also be carefully drafted. If this field is retained, it should refer to the controller’s responsibility for the notification and should not require a personal declaration by the DPO, reporting person, or other individual unless required by applicable national procedural law. The template should also avoid requesting national identification numbers except where strictly required by national law and demonstrably necessary for the supervisory authority’s processing of the notification.

3. The Template should preserve the Risk-Based thresholds in Articles 33 and 34 GDPR

The template should clearly separate the Article 33 notification assessment from the Article 34 communication assessment. Article 33 concerns notification to the supervisory authority where the breach is likely to result in a risk to the rights and freedoms of natural persons. Article 34 concerns communication to data subjects where the breach is likely to result in a high risk to their rights and freedoms .

We welcome the template’s inclusion of an outcome field for the controller’s risk assessment, including the options that the breach is likely to result in high risk, likely to result in non-high risk, unlikely to result in risk, or that additional information is needed. We recommend, however, that the template add clearer guidance explaining that not every personal data breach is notifiable to the supervisory authority and that not every notifiable breach must be communicated to data subjects.

An additional idea here is to include the highly welcomed information of the EDPB (Guidelines 9/22 and 1/21) into the form servers. Especially the search of examples would help to create a comprehensive analyses of the resulting risks of an incident, that should possibly need to be notified.

We also recommend that the template include a short, practical explanation of the difference between “risk” and “high risk,” and that it allow controllers to document uncertainty without prejudicing their position. In practice, controllers may notify early out of caution while expressly reserving the outcome of their investigation. The template should support that approach and should not treat an incomplete risk assessment as a failure to comply.

4. The Template Should Avoid Over-Collection of Personal Data

The template itself should embody data minimization. Several fields may lead to the collection of personal data about reporting persons, contact persons, DPOs, representatives, employees, or affected individuals. We recommend that the EDPB assess whether each field is necessary and proportionate for the purpose of breach notification.

In particular, fields requesting the national identification number of the reporting person should be omitted from the common template unless a specific national supervisory authority has a legal requirement for such information. If retained, the field should be disabled by default and activated only in Member States where it is legally required. Similarly, the template should discourage inclusion

of unnecessary personal data in free-text fields, attachments, screenshots, forensic reports, phishing messages, communications to data subjects, or other supporting documents.

The attachments section should include a warning that controllers should redact or exclude personal data that is not necessary for the supervisory authority's assessment. This is especially important for phishing emails, ransomware notes, screenshots, logs, mailbox exports, and forensic reports, which may contain personal data of employees, customers, or third parties.

5. Free-Text Fields Should Be Supported by Clear Guidance and Examples

The template contains several important free-text fields, including descriptions of the breach, discovery, timeline, systems and infrastructure, risk assessment methodology, likely consequences, measures taken, and measures to prevent recurrence. These fields are necessary, but they may generate inconsistent submissions unless accompanied by clear guidance.

We recommend that the final template include concise examples of appropriate levels of detail for different incident types, such as misdirected email, ransomware, compromised mailbox, lost device, unauthorized internal access, public cloud misconfiguration, and processor-originated breach. These examples should be practical and should distinguish between information expected in an initial notification and information expected in a follow-up notification. For example, in a misdirected email scenario, the initial notification might state that a payroll file was sent to one unintended recipient, identify the categories of data contained in the file, confirm whether the recipient has been asked to delete the email, and explain whether there is any evidence of onward disclosure. A follow-up notification could then confirm whether deletion was verified, whether additional recipients were identified, and whether any affected employees were informed.

The guidance should also encourage controllers to identify assumptions, uncertainties, and pending investigation steps. For example, where exfiltration is suspected but not confirmed, the controller should be able to state the factual basis for that assessment without being forced into a definitive conclusion prematurely. In a ransomware scenario, the initial free-text fields should allow the controller to state, in the breach description field, that specified systems were encrypted and that forensic analysis is ongoing; in the likely consequences field, whether critical services are unavailable and whether any ransom note claims exfiltration; and in the measures taken/preventive measures field, whether backups are available and what containment or restoration steps have been initiated. The follow-up free-text fields should then allow the controller to confirm, in the breach description field, the root cause and duration of service unavailability; in the affected systems and records field, the systems and datasets confirmed to be affected; in the risk assessment field, whether logs or forensic findings indicate exfiltration; and in the measures taken/preventive measures field, the recovery measures completed and any additional measures adopted to prevent recurrence. In a compromised mailbox scenario, the initial free-text fields should allow the controller to identify, in the breach description field, the mailbox and approximate period of compromise; in the breached data field, the categories of messages or attachments potentially affected; in the measures

taken/preventive measures field, immediate containment steps such as password reset and session revocation; and in the risk assessment field, the fact that mailbox review remains pending. The follow-up free-text fields should allow the controller to provide, in the breach description field, the results of the mailbox review and whether forwarding rules, downloads, or other suspicious activity were identified; in the categories and number field, the categories and approximate number of affected data subjects; in the risk assessment field, the updated assessment based on the mailbox review; and in the communication to data subjects field, whether communications were required or completed. In a lost device scenario, the initial free-text fields should allow the controller to state, in the breach description field, the type of device and circumstances of loss; in the measures in place field, whether the device was encrypted or protected by access controls; in the measures taken/preventive measures field, whether remote wipe or mobile device management controls were activated; and in the breached data field, the categories of data believed to be stored locally. The follow-up free-text fields should allow the controller to confirm, in the measures taken/preventive measures field, whether the device was recovered or wiped; in the measures in place field, whether encryption and access controls were verified; in the likely consequences field, whether any data were accessible without credentials; and in the risk assessment field, whether the controller's assessment changed after technical verification.

6. Cross-Border Processing Fields Should Be Clarified

The template includes fields concerning cross-border processing, lead supervisory authority, countries where the controller has establishments, countries where affected data subjects are located, and supervisory authorities notified or to be notified. We support the inclusion of these fields, because they can assist cooperation among supervisory authorities. However, these fields should be designed so that controllers are not required to resolve complex one-stop-shop issues before submitting a timely initial notification.

We recommend that the template allow controllers to select "unknown," "under assessment," or "to be confirmed" for the lead supervisory authority and affected countries during an initial notification. The template should also clarify that notifying a supervisory authority through the template does not itself determine the lead supervisory authority, the existence of cross-border processing, or the allocation of competence among supervisory authorities.

The template should further clarify how it applies to controllers not established in the EEA but subject to the GDPR. The section on non-EEA establishments is helpful, but the final template should provide practical guidance on how such controllers should identify relevant supervisory authorities and affected Member States where the facts remain incomplete.

7. Processor and Joint Controller Scenarios Need More Granular Treatment

The template asks whether other parties such as processors or joint controllers are involved and requests identification and contact details. We recommend expanding the guidance for this section,

because breach reporting frequently involves complex factual chains involving processors, sub-processors, joint controllers, cloud providers, managed service providers, cybersecurity vendors, and group companies.

The template should distinguish between the party whose systems were affected, the party that discovered the incident, the controller responsible for notification, the processor that notified the controller under Article 33(2), and any joint controller or separate controller whose processing may also be implicated. This would improve the quality of notifications and reduce confusion in multi-party incidents. For example, in a managed payroll service incident, the payroll provider's platform may be affected, the provider may discover and contain the incident, the employer may remain the controller for employee data, and another group company may act as a separate controller for expatriate employee records. The template should allow those roles to be described distinctly rather than forcing all parties into a single "other party" category.

Where the incident originates at a processor, the template should allow the controller to state which information has been received from the processor and which information remains pending. This is important because controllers often depend on processors for technical facts necessary to complete the notification. For example, where a cloud email provider informs a controller that a mailbox was compromised, the controller may initially know the mailbox owner, the approximate period of compromise, and the fact that message rules were created, but may not yet know whether attachments were accessed, which data subjects were affected, or whether the provider has completed its log review. The template should permit the controller to submit that partial information without implying that the controller has failed to investigate.

8. <u>The Template Should Reduce the Risk of Defensive or Excessive Reporting</u>

A common template should encourage timely and meaningful notification, but it should not incentivize defensive over-reporting or excessive submission of documents. The current level of detail, if implemented rigidly, may cause controllers to submit incomplete notifications for incidents that may ultimately be unlikely to result in risk, simply because the process appears to require extensive documentation once an incident is being assessed.

We recommend that the template include a clear preliminary triage pathway. This pathway should allow controllers to record that an event has been assessed and is unlikely to result in risk, where they choose to document the assessment internally rather than notify. If the EDPB considers that the template should only be used for notifications actually submitted to supervisory authorities, it should nevertheless make clear in the guidance that controllers are not expected to notify every security incident.

9. <u>Risk Based Templates</u>

DPAs complain about a huge amount of the more simple cases like incorrect addressing cases, phishing with only possible but not verified access to a mailbox or lost data storage devices etc. We

see an option of thinking about simplified notification templates and a simplified process. In these known cases it would be helpful to ask specific additional questions to identify the risk and guide the investigation of the controller.

10. Communication to Data Subjects Should Be Handled Flexibly

The template's section on communication to data subjects is useful, particularly where data subjects have already been informed or where Article 34(3) GDPR is relied upon. Article 34 requires communication to data subjects where the breach is likely to result in a high risk, and it sets out exceptions where communication is not required, including where appropriate technical and organizational protection measures were applied, subsequent measures ensure that the high risk is no longer likely to materialize, or communication would involve disproportionate effort .

We recommend that the template recognize phased communications, targeted communications to different categories of data subjects, and situations where communication content evolves as the investigation develops. For example, in a compromised mailbox incident, the controller may first notify the mailbox owner and internal employees whose data is confirmed to be affected, then notify customers or suppliers after mailbox review identifies relevant messages or attachments, and later issue a public notice if individual contact details are incomplete. The template should allow the controller to describe those phases, the categories covered by each phase, and the expected timing of any remaining communications. The template should also allow controllers to provide a representative version of communications rather than full individualized communications where the latter would involve unnecessary personal data or operational burden.

The field requesting the content of the information provided to data subjects should include guidance that controllers may provide templates, versions, or redacted examples where appropriate. For example, where a bank sends different versions of a notice to customers whose payment card details were affected and to customers whose contact details alone were affected, the template should allow the controller to upload or reproduce representative versions for each group, rather than requiring individualized copies of every communication. This would support supervisory assessment while avoiding unnecessary disclosure of personal data or sensitive incident details.

11. Attachments Should Be Optional and Proportionate

The attachments section lists several categories of documents, including communications to data subjects, risk assessments, research reports, ransomware notes, phishing messages, internal procedures, deletion policies, communications to wrong recipients, and external notifications. These documents may be relevant in some cases, but requiring or encouraging broad attachment of incident materials may create unnecessary risks.

We recommend that attachments remain optional unless specifically requested by the supervisory authority or necessary to understand the notification. The template should include guidance that attachments should be limited to what is relevant, proportionate, and safe to disclose. It should also

recommend redaction of personal data, security-sensitive information, credentials, tokens, malware indicators that could create risk if mishandled, and third-party confidential information where not necessary for the supervisory authority's assessment.

The phishing-specific tooltip is helpful, but it should be generalized into broader guidance on attaching incident artifacts safely. For example, compromised mailbox material, screenshots, log files, forensic exports, and ransomware communications should not be uploaded wholesale unless necessary and appropriately sanitized.

12. Accessibility, Multilingual Availability, and Interoperability Should Be Prioritized

The template will be most useful if implemented consistently across supervisory authorities and made available in all official EU languages, while preserving a common data model. We recommend that the EDPB publish a machine-readable schema for the template, including field names, definitions, mandatory status, conditional logic, and controlled vocabularies. This would allow controllers, DPO teams, incident response vendors, and case management tools to prepare notifications more efficiently.

The EDPB should also clarify whether supervisory authorities will implement the template as a unique template, as a meta-template, or through compatible national forms. The public consultation page states that, following consultation, the EDPB will decide on the timeline for practical implementation by all DPAs. A common implementation roadmap would help organizations prepare internal breach reporting workflows and ensure consistency across Member States.

For internal preparation and for transparency of the process it is helpful to provide the template as a document file, independent from an online form. This file can be used for internal preparation of a notification, as well as be used as a basis for internal documentation, when it comes to the decision of not to notify.

13. The Template Should Be Tested with Realistic Incident Scenarios

Before finalization, we recommend that the EDPB test the template against realistic breach scenarios involving organizations of different sizes and maturity levels. These should include a microenterprise misdirected email incident, a hospital ransomware incident, a processor-originated cloud incident, a multinational cross-border breach, a compromised mailbox with uncertain exfiltration, a lost encrypted device, and an incident involving non-EEA controllers subject to the GDPR.

Such testing would help identify fields that are unclear, duplicative, unavailable in practice, or likely to cause delayed notification. It would also help ensure that the template supports both simple and complex breaches without imposing the same level of burden on all notifications.

14. Specific Drafting and Technical Recommendations

We recommend that the EDPB consider the following concrete amendments.

a. The template should add an introductory statement explaining that even if a DPO notifies the breach the controller remains responsible for determining whether a breach is notifiable under Article 33 GDPR and whether communication to data subjects is required under Article 34 GDPR.
b. The template should mark fields as “Article 33 required,” “recommended,” “optional,” or “follow-up,” rather than using only mandatory and conditional mandatory labels. We understand the idea that for the creation of dataset that can be analysed these fields would be helpful, but it should be checked whether these are within the scope of Art. 33 GDPR.
c. The template should provide a “not yet known” or “under assessment” option wherever information may reasonably be unavailable within 72 hours, including for affected countries, number of data subjects per country, lead supervisory authority, exfiltration assessment, root cause, systems affected, and measures to prevent recurrence.
d. The template should remove the national identification number field from the common template or restrict it to Member States where required by law.
e. The template should clarify that naming a DPO as a contact point does not make the DPO personally responsible for the controller’s notification or assessment.
f. The template should introduce a security and data minimization warning for free-text fields and attachments.
g. The template should provide examples for the most common incident types and indicate what level of detail is expected at initial and follow-up stages. There even might be templates, they may populate the form from the examples.
h. The template should include a machine-readable schema and implementation guidance for organizations and supervisory authorities.
i. The template should clarify that attachment of internal policies, forensic reports, phishing messages, or communications should be limited to what is necessary and proportionate. An information is needed so that the notifier understands that information mainly should lead to an easy and quick understanding of the case.
j. The template should clarify how withdrawals are to be handled, including where an initial notification was made out of caution and subsequent assessment indicates that the event is unlikely to result in risk. This could be especially helpful if it is likely that someone is raising the case at the DPA. The controller has the chance to document that the notification was considered and that the case was thoroughly investigated.

15. <u>Recommendations for the process of the notificaation</u>

For the technical notification systems problems with time-outs are visible: this kind of an extensive form needs quite some time to fill it in. During the time frame for completing the form interruptions are likely (e.g. an incoming phone call). Think of the situation of the occurrence of the incident, where the internal investigation and reaction has priority. The current state should not get lost and be recoverable. Time-Outs are a recurring problem at the notification platforms.

The processing of the notification at the DPAs differs highly. There is sometimes no acknowledgement about the successful submission. Especially for sporadic users it is not clear how the notification is processed, which stages there are in the process. There should be Transparency about the state of process.

Large organisations tend to submit reports more frequently, so that saving default settings can both facilitate allocation by the data protection supervisory authority and significantly speed up the processing of the report by the reporting organisation.

Notification with a registration would help in both directions: general data of the organisation can be pre-set; the data protection supervisory authority can reliably ensure that notifications are clearly assigned to the same data controller.

Conclusion

The EFDPO Association strongly supports the EDPB's effort to harmonize personal data breach notification practice across the EEA. A common template can materially improve consistency, reduce administrative friction, and support timely communication between controllers and supervisory authorities. To achieve those benefits, however, the final template should remain proportionate, risk-based, and workable during the first 72 hours of an incident.

We therefore encourage the EDPB to refine the template by narrowing mandatory fields for initial notifications, clarifying the role of the DPO, strengthening data minimization safeguards, improving guidance for uncertainty and follow-up notifications, and ensuring that implementation is interoperable across supervisory authorities. These changes would enhance the template's practical value while preserving the legal structure and risk-based approach of the GDPR.

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

EFDPO contacts:

EFDPO Press Office, phone +49 30 20 62 14 41, email: office@efdpo.eu,

President: Thomas Spaeing (Germany)

Vice Presidents: Xavier Leclerc (France), Judith Leschanz (Austria), Inês Oliveira (Portugal), Vladan Rámiš (Czech Republic)

About EFDPO

The European Federation of Data Protection Officers (EFDPO) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The association is based in Brussels.

Members:

- Austria: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at
- Czech Republic: Spolek pro ochranu osobních údajů
- Finland: Finnish Data Protection Association (Tietosuoja ry)
- France: UDPO, Union des Data Protection Officer - DPO
- Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
- Greece: Hellenic Association for Data Protection and Privacy (HADPP)
- Hungary: Hungarian Association for Data Protection Awareness, MADAT (Magyar Adatvédelmi Tudatosságért Társaság Egyesülete)
- Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
- Norway: Norwegian Association of Data Protection Officers (in Norwegian: *Foreningen Personvernombudene*)
- Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
- Slovakia: Spolok na ochranu osobných údajov
- Switzerland: DAPRI Data Privacy Community