CEDPO Contribution on the EDPB Draft Template for Personal Data Breach Notification

Public Consultation Response

05/08/2026

CEDPO welcomes the European Data Protection Board's initiative to develop a common template for the notification of personal data breaches. A harmonised template has the potential to improve legal certainty, facilitate compliance with Article 33 GDPR and significantly reduce the operational burden faced by controllers and Data Protection Officers, particularly in the context of cross-border incidents.

CEDPO particularly welcomes the template's risk-based structure, the use of conditional fields and business logic, the possibility of submitting incomplete initial notifications, and the intention to implement the template through digital tools.

For these benefits to materialise, however, the template must be implemented consistently across the EEA, remain proportionate to the requirements of Article 33 GDPR, and avoid unnecessary duplication between national, European and sector-specific reporting procedures. CEDPO's comments below aim to contribute to improving the template's legal clarity, practical usability and interoperability.

General Remarks

CEDPO supports the objective of harmonising personal data breach notification practices across the EEA. The effectiveness of the initiative would nevertheless be significantly reduced if supervisory authorities retained substantially different notification processes or introduced additional mandatory national fields.

CEDPO therefore recommends that the EDPB:

- establish a clear and coordinated implementation timetable;
- encourage supervisory authorities to use the common template without additional mandatory national requirements, except where strictly required by applicable law;
- distinguish clearly between information required to satisfy Article 33 GDPR and supplementary information that may assist a supervisory authority;
- ensure that supplementary governance information and supporting documents remain optional;
- provide for interoperable technical implementation, including conditional fields, pre-population, machine-readable formats and the reuse of information already submitted.
- facilitate the submission and management of cross-border notifications through coordinated technical and procedural arrangements.

The template should also expressly clarify that it provides a structured means of complying with the notification obligation under Article 33 GDPR and is not intended to extend or restrict the scope of that obligation.

1. Scope and Legal purpose of the Template

The common template should remain focused on the notification obligation established by Article 33 GDPR.

Article 33 requires the controller to notify the competent supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. It also identifies the minimum categories of information to be communicated and allows information to be provided in phases where it cannot be supplied at the same time.

CEDPO recommends adding a clear statement to the introduction explaining that the template:

- structures the information required for the purposes of Article 33;
- does not create new substantive notification obligations;
- does not alter the legal threshold for notifying a breach;
- does not make supplementary governance measures or documents mandatory unless required under the GDPR or other applicable law;
- does not prevent supervisory authorities from requesting further information subsequently where this is necessary and proportionate.

This clarification is important because certain fields could otherwise be interpreted as requiring controllers to provide information that goes beyond what is necessary for an initial breach notification.

The template should facilitate compliance rather than transform the notification process into a broader audit of the controller's data protection and cybersecurity governance.

2. Mandatory and Optional Information

The Draft Template's distinction between mandatory, conditionally mandatory and optional fields is generally appropriate. CEDPO nevertheless recommends a limited number of adjustments to ensure that additional explanations are only required where they are relevant.

In particular:

- field 51 should only require a further description of how the breach was discovered where "Other" is selected or where an explanation is needed to clarify the controller's awareness of the breach;
- field 66 should only be mandatory where additional categories of data subjects are identified or further information on vulnerability is required;
- field 71 should only be mandatory where additional data types are selected or clarification is otherwise necessary;

- field 76 should only require a detailed description where the preceding answers indicate that further explanation of the protective measures is relevant;
- fields 117 and 122 should allow the controller to indicate that the number of affected data subjects per country is not yet reasonably available and will be supplied in a follow-up notification;
- field 105 should be mandatory where “Other” is selected as the means used to communicate the breach to data subjects.

CEDPO recommends aligning the business logic for these fields accordingly. Information that is not reasonably available at the time of notification should be capable of being provided through a follow-up notification in accordance with Article 33(4) GDPR.

3. Conditional fields and digital usability

CEDPO welcomes the use of conditional fields and business logic.

The digital form should only display questions that are relevant to the circumstances of the notification and should avoid requesting the same information more than once.

In particular:

- DPO details should not be requested again where the DPO is already identified as the reporting person;
- information entered in an initial notification should be retained in follow-up notifications;
- previously supplied controller and contact information should be reused;
- the organisation should be able to save, review and export its submission.

Common technical rules should be developed to avoid different national implementations of the same template.

4. Pre-population and Machine-readable Formats

CEDPO supports the pre-population of reliable information already held by public authorities.

For example, the controller’s identification details could be retrieved after the organisation provides a valid company or organisation number. DPO information could also be retrieved from an official designation register where such a register exists.

All pre-populated information should remain subject to verification and correction by the controller.

The EDPB should also promote secure APIs and machine-readable formats so that organisations can import information from existing incident-management systems rather than re-entering it manually.

5. Incomplete and Follow-up Notifications

CEDPO welcomes the possibility of submitting an incomplete notification.

The template should clarify that the controller is required to provide the relevant information reasonably available at the time of notification. Information that remains under investigation may be supplied through a follow-up notification.

A completed forensic investigation should not be treated as a prerequisite for notification. The precise attack method, root cause, affected systems or number of individuals may not yet be known within 72 hours.

The technical implementation should allow the controller to reopen and supplement the existing notification. Previously submitted information should be pre-populated and remain editable where it needs to be corrected or updated.

6. Withdrawal of a Notification

CEDPO welcomes the possibility of withdrawing a previous notification.

The EDPB should nevertheless clarify:

- whether withdrawal closes the notification procedure;
- whether the original notification is retained and for how long;
- whether the controller will continue to have access to it;
- whether the supervisory authority may continue examining the incident;
- whether further information may still be requested;
- how the withdrawal will be recorded.

The controller should receive confirmation that the withdrawal has been registered and should understand the resulting procedural status of the notification.

7. Risk Assessment

CEDPO welcomes the risk-based structure of the Draft Template.

However, harmonisation of the notification form may remain incomplete unless controllers and supervisory authorities have a sufficiently consistent understanding of how risks to the rights and freedoms of individuals should be assessed.

CEDPO therefore invites the EDPB to provide further practical guidance, criteria or examples supporting a more consistent assessment across the EEA.

In particular, the relationship between the following fields should be clarified:

- field 87, concerning the severity of the potential impacts; and
- field 89, concerning the overall outcome of the risk assessment.

These fields should not appear to request the same assessment twice. The template should explain that the severity of a potential impact is one element of the overall risk assessment and must be considered together with the likelihood that the impact will materialise and any relevant mitigating circumstances.

Field 90, which asks the controller to describe the methodology and relevant factors considered, could refer to common EDPB guidance or examples where available.

8. Internal Reference Number

CEDPO supports retaining field 7, which allows the controller to provide its internal reference number.

Such a reference may facilitate follow-up exchanges and connect the notification with the controller's internal documentation.

The field is currently optional, which appears appropriate. Controllers could be encouraged to complete it where an internal reference has been assigned, without making it a condition of a valid notification.

9. Role of the Controller and the DPO

The template should clearly reflect that responsibility for complying with Article 33 GDPR remains with the controller.

The DPO may advise the controller, contribute to the assessment, act as a contact point and submit the notification where authorised to do so. However, the form should not suggest that the DPO personally assumes the controller's responsibility for the notification.

CEDPO recommends amending the relevant option in field 23 to read:

DPO, where authorised by the controller to submit the notification.

Where the reporting person is already identified as the DPO, fields 29–31 should not request the same information again.

Where reliable DPO designation records exist, the relevant information could be pre-populated, subject to verification and correction by the reporting person.

10. National Identification Number

Field 25 provides for the possible collection of the reporting person's national identification number. The Draft Template indicates that this field is optional and should only be implemented where required.

CEDPO nevertheless invites the EDPB to clarify that the field should only be implemented where:

- a specific legal basis requires the identifier;
- its collection is strictly necessary for the notification process; and
- no less intrusive identification method is reasonably available.

A national identification number should not be requested merely for administrative convenience.

This clarification would help avoid unnecessary or inconsistent implementation by national supervisory authorities.

11. Systems, Software and Infrastructure

CEDPO recognises that information about the systems, software, services and infrastructure involved may be necessary to understand the nature and scope of a personal data breach.

However, field 63 should require only a proportionate description of the systems materially involved in the incident. It should not be interpreted as requiring a comprehensive description of the controller's IT environment.

The tooltip should also remind controllers not to disclose unnecessarily:

- detailed network architecture;
- credentials or encryption keys;
- exploitable vulnerability information;
- information about unaffected systems;
- other confidential or security-sensitive technical information.

Where more detailed technical information is required, it should be requested separately and transmitted through an appropriately secure channel.

12. Number of Affected and Informed Data Subjects

Number of affected data subjects

CEDPO welcomes the possibility, under fields 67 and 68, of providing either an exact or an approximate number of affected data subjects.

This flexibility is particularly important where the full scope of the personal data breach is still being investigated at the time of the notification.

The template should continue to allow controllers to:

- provide a reasonable estimate where an exact number is not yet available;
- explain, where relevant, the basis of that estimate; and
- update the number through a follow-up notification.

Communication to data subjects

CEDPO also supports retaining field 102, which asks whether all affected data subjects have been informed.

However, the template should better address situations in which the controller communicates the breach through a public announcement, website notice or similar measure. In such cases, the controller may be unable to determine how many affected individuals actually received or viewed the information.

The available answers or tooltip should therefore allow the controller to indicate that:

- a public communication or similar measure was used;
- the precise number of data subjects reached cannot reasonably be determined; or

- the communication process is still ongoing.

Controllers should not be expected to introduce tracking technologies or carry out additional processing solely to estimate how many individuals viewed a public notice.

13. Notifications to Other Authorities and Bodies

CEDPO supports retaining fields 109–111 concerning reports or notifications to police, judicial authorities and other supervisory or regulatory bodies.

These fields appropriately allow the controller to indicate whether another report or notification has been made and, where applicable, to identify the authority or body concerned and provide the relevant case reference. They may facilitate coordination where the same incident is subject to several reporting regimes.

CEDPO nevertheless notes that controllers, DPOs and incident-response teams may be required to submit substantially similar information through several data protection, cybersecurity or sector-specific portals.

CEDPO therefore encourages the EDPB to promote technical interoperability and the secure reuse of information already submitted, including through common data formats and appropriate interfaces.

In the longer term, a more integrated reporting mechanism could reduce repetitive manual input and improve consistency. Any development towards a single-entry service would, however, need to preserve the distinct legal thresholds, deadlines, competent authorities and confidentiality requirements applicable under each reporting regime.

14. Cross-border Notifications

CEDPO supports further simplification of the notification process where a personal data breach concerns several EEA countries or supervisory authorities.

Fields 118 and 123 ask the controller to identify the EEA supervisory authorities to which the breach has been or will be notified. The Draft Template does not specify whether these fields are purely declaratory or whether the future IT implementation may facilitate transmission of the notification to the authorities concerned.

CEDPO invites the EDPB to clarify this point as part of the practical implementation of the template.

Where legally and technically feasible, cooperation and secure information exchange between supervisory authorities could reduce the need for controllers to submit substantially identical information through several national portals.

CEDPO also notes that “EAA supervisory authority” in field 123 should be corrected to “EEA supervisory authority”.

15. Attachments and Supporting Documents

CEDPO welcomes the fact that field 125 concerning attachments is optional.

The documents listed in this field may nevertheless contain personal data, confidential or security-sensitive information, or information protected by professional secrecy or applicable legal privilege.

CEDPO therefore recommends adding guidance reminding controllers to assess the necessity and content of an attachment before submitting it. Where appropriate, controllers should be able to provide:

- a redacted version;
- a relevant extract;
- a factual summary; or
- an explanation that the document cannot be provided in full because of confidentiality, security or privilege concerns.

Where additional documentation is necessary, the supervisory authority should be able to request it subsequently and through an appropriately secure channel.

Summary of Recommendations

CEDPO recommends that the EDPB:

1. Clarify the legal purpose and scope of the common template.
2. Adjust the business logic of specific fields where further explanations should only be conditionally mandatory.
3. Ensure consistent use of conditional fields and avoid duplicate data entry.
4. Enable verified pre-population and the use of secure, machine-readable formats.
5. Clarify that information not reasonably available may be provided through follow-up notifications.
6. Explain the procedural consequences of withdrawing a notification.
7. Provide further guidance on the risk assessment and clarify the relationship between fields 87 and 89.
8. Retain the optional internal reference field and encourage its use where a reference has been assigned.
9. Confirm that responsibility for the notification remains with the controller and that the DPO may submit it where authorised.
10. Clarify the limited circumstances in which a national identification number may be requested.
11. Limit field 63 to a proportionate description of the systems materially involved and address the protection of confidential and security-sensitive information.
12. Maintain the flexibility to provide an approximate number of affected data subjects and adapt field 102 to public communications where the number of persons reached cannot reasonably be determined.
13. Retain fields 109–111 and promote interoperability with other incident-reporting systems.

14. Clarify whether fields 118 and 123 are purely declaratory or may support transmission or cooperation between supervisory authorities in the future IT implementation.

15. Keep attachments optional and provide guidance on redaction, confidentiality, security and applicable privilege.

Closing Observations

CEDPO welcomes the Draft Template as an important step towards more consistent personal data breach notification procedures across the EEA.

Its practical value will depend on proportionate information requirements, consistent implementation by supervisory authorities and digital tools that reduce unnecessary duplication.

CEDPO encourages the EDPB to retain the positive features of the Draft Template while providing the clarifications and targeted adjustments identified in this contribution.