Spolek pro ochranu osobních údajů

Comments on the EDPB draft Template for personal data breach notification

We welcome the opportunity to provide feedback on the recently published EDPB draft of Template for personal data breach notification ("Template").

We appreciate the considerable work undertaken and the effort to harmonise the structure of notifications submitted to supervisory authorities in the individual Member States. A common European notification structure may increase legal certainty for controllers, facilitate the work of data protection officers and incident response teams, and enable supervisory authorities to process notifications more efficiently.

However, we consider that, in its current form, the draft primarily represents a highly detailed standardisation of the information requested, rather than a simplification of the notification process.

In practice, notifications under Article 33 GDPR are often submitted at a time of considerable uncertainty, under time pressure and in parallel with technical investigations, system recovery, communication with data subjects and compliance with notification obligations under other legislation. This places a significant strain on the affected controller's resources and depletes them. Those resources should therefore not be further and disproportionately burdened by extensive information requirements in the initial phase of the breach investigation vis-à-vis supervisory authorities, particularly in situations where the supervisory authorities cannot be always expected to provide practical assistance to the affected controller.

We therefore recommend revising the draft, in particular with regard to proportionality, phased notification, interoperability with other regulatory regimes and the practical usefulness to supervisory authorities of the information requested.

We also recommend conducting a practical pilot test of the template before its final adoption, involving data protection officers, incident response teams, small and medium-sized enterprises, large multinational organisations and representatives of supervisory authorities. Such testing could show which information is genuinely available within the 72-hour period and which data supervisory authorities actually need for their immediate response.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: +420 730 677 644

Spolek pro ochranu osobních údajů

General comments on the template

Phased notification

In our view, the template should be designed from the outset as reflecting the phased notification process.

Under Article 33(3) GDPR, the “initial” notification to the supervisory authority must "at least" include:

1. A description of the nature of the personal data breach, including where possible the categories and approximate number of data subjects and records concerned.
2. The name and contact details of the DPO or other contact point.
3. A description of the likely consequences of the breach.
4. A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects.

Where some of these elements are unknown at the time of the initial notification, the controller should provide what it can and then supplement the record in later phases as the investigation progresses. When the controller first notifies the supervisory authority, it should also inform the authority that it does not yet have all the required information and will provide more details later on.This does not prevent the controller from providing further information at any other stage of the investigation, if it becomes aware of additional relevant details that need to be communicated to the supervisory authority.

The initial notification submitted within 72 hours should therefore contain only a limited set of basic information that is actually known to the controller at that time or that the controller can establish without disproportionate effort (see also Article 33(4) GDPR). This should principally cover the basic elements envisaged in Article 33(3), but should allow for a narrative description rather than requiring a highly segmented form.

A detailed technical, factual and legal assessment could be provided in a subsequent notification pursuant to Article 33(4) GDPR. This approach should not be regarded as an exception or as a deficiency in the initial notification, but as the standard approach appropriate to more serious security incidents. It would also be helpful if the supervisory authority itself indicated to the controller whether it wished to receive a more detailed report at a later stage. For various reasons, the supervisory authority will often be unable to examine the case in greater detail, in which case it is not reasonable to divert the controller's resources to submitting additional information that will not be used.

An excessively detailed mandatory form may also have significant unintended effects: controllers may delay notification until they have obtained sufficient information, or may be reluctant to submit a notification containing preliminary data that later prove inaccurate. The template should instead encourage prompt initial notification and allow the information to be progressively refined.

We therefore recommend dividing the fields into:

1. mandatory fields for the basic initial notification, reflecting Article 33(3) GDPR;
2. fields intended for subsequent notifications;
3. optional fields that controllers may complete where the information is already available;
4. information that the supervisory authority may subsequently request on an individual basis where needed for the particular case.

Coordination with other notification regimes and reporting on behalf of multiple controllers

A serious cybersecurity incident may simultaneously be subject to notification obligations under the GDPR, the NIS2 Directive, the DORA Regulation, sector-specific legislation and, where applicable, obligations vis-à-vis the police, insurers or contractual partners. These regimes often use different time limits, terminology and reporting structures.

When finalising the template, the EDPB should seek to apply the 'once-only' principle consistently (see also the Digital Omnibus proposal) and coordinate the form as closely as possible with other authorities so that it may serve as a universal reporting instrument; see, for example, the parallel efforts to coordinate forms under NIS2.[1]

The template should therefore use a machine-readable and jointly coordinated data model that individual public authorities can incorporate into their systems.

It would also be important to confirm the EDPB's position in Guidelines 9/2022, namely that a controller engaged in cross-border processing should notify only its lead supervisory authority.

In practice, incidents quite often originate with a processor used by a large number of controllers. The template could therefore also address such cases and introduce procedures enabling simplified reporting by controllers responding to a cybersecurity incident that has already been reported by 'their' processor under its obligations pursuant to other legislation, such as NIS2 - for example, by allowing them to refer to the reference number of that report.

We would also regard it as a significant benefit if the electronic tool included a module capable of helping controllers make a preliminary assessment of whether an incident may be subject to a notification obligation and under which legislation.

Comments on individual fields

1. **Field 26 - 'Accuracy & Responsibility'**

The meaning of the 'Accuracy & Responsibility' field is not sufficiently clear to us.

We recommend either deleting this field or defining its purpose precisely. In particular, given the situation described above, where the information submitted is that available at the relevant time, the use of such a field - which is itself somewhat unclear - may be problematic.

[1] https://digital-strategy.ec.europa.eu/cs/news/nis2-cooperation-group-adopts-common-templates-incident-reporting

2. **Fields 38 to 41 - involvement of other entities**

We welcome the possibility of identifying processors, joint controllers and other entities involved in the incident.

However, the template could also allow several joint controllers to submit a single joint notification on a voluntary basis (for example, where their arrangement under Article 26 does not specify that only one of them is to submit the notification).

3. **Fields 51, 52 and 61 - detection and cause of the incident**

A detailed description of how the incident was detected and its cause identified may not be available at the time of the initial notification. In complex cybersecurity incidents, a forensic investigation may take weeks or months.

Field 51 should therefore not be mandatory in the initial notification phase beyond brief information on how the incident was detected. A detailed description of the detection mechanism may also contain security-sensitive information.

For Field 52, we recommend allowing the answers 'not yet established' or 'to be provided'. The date on which another person, in particular a processor, notified the incident may be relevant to the timeline, but should not automatically support a conclusion that the notification was late or that obligations were breached.

In our view, the mandatory classification in Field 61 of the cause of the incident as internal or external and intentional or unintentional is also problematic. During the initial stages of an investigation, it may be impossible to identify the perpetrator or determine their intent. In particular, the label 'internal malicious' may raise issues relating to the privilege against self-incrimination and to the controller's potential criminal or administrative liability.

We therefore recommend:

- allowing the answer 'under investigation' in subsequent notifications as well;
- making the detailed classification of the cause optional;
- expressly stating that a preliminary classification may subsequently be changed;
- not drawing adverse conclusions solely because the cause has not yet been determined;
- respecting the applicable rules on the privilege against self-incrimination.

4. **Closed lists of answers**

Incidents often involve a combination of several causes, types of breach and impacts. As a rule, the form should therefore allow multiple selections.

The following options should also be available in all relevant closed lists:

- 'Other - please specify';

- 'Cannot be determined';
- 'Under assessment';
- 'Not applicable'.

These options should not be limited to preliminary notifications where a particular fact objectively cannot be established even after the investigation has been completed. In some cases, 'cannot be determined' is a legitimate outcome of an investigation and should not be regarded as inadequate cooperation by the controller.

5. Fields 67, 68, 72 and 73 - number of affected data subjects and records

At the initial stage of an incident, the controller often does not know the exact or even approximate number of affected data subjects. For example, it may know only the volume of data in GB exfiltrated from a particular system, without being able to determine the number of unique individuals or the precise categories of data.

The controller should provide its best informed estimate only where it can do so on the basis of reasonably available information.

The requirement to state the number of individual personal data records is particularly problematic. The term 'record' is not used consistently across different information systems. A single database row may contain many data items concerning one person, while information concerning one person may be distributed across hundreds of tables, files, emails or logs. Requiring the number of individual records may therefore produce figures that appear precise but are not in fact comparable.

More precise quantification should be provided subsequently, but only where technically feasible and proportionate.

6. Fields 75 and 76 - measures in place before the incident

The requirement to provide a detailed list of measures in place before the incident goes beyond the basic content of a notification under Article 33(3) GDPR. Such information may be relevant to subsequent supervisory action by the supervisory authority, but is generally not necessary for assessing the notification (see, for example, the possible conflict with the privilege against self-incrimination noted above).

Complex incidents also usually involve a combination of technical and organisational measures. Without knowing the specific system architecture, it is impossible to infer merely from whether individual boxes are ticked whether the level of security was appropriate.

We therefore recommend that this section be optional in the initial notification phase or limited to measures directly relevant to the occurrence and impact of the particular incident, where known at the relevant time (although, in practice, accurately identifying the measures relating to a particular incident may be problematic, especially in case of using large processors). The supervisory authority should, for example, be able to request detailed information subsequently on an individual basis if it needs that information to assess the incident.

The form should also expressly state that failure to indicate one of the listed measures does not automatically mean that the controller did not have that measure in place or was required to implement it in view of the nature of the processing.

7. **Field 79**

A preliminary description of the likely consequences and the measures taken to mitigate the incident forms part of the content of a notification under Article 33 GDPR. The level of detail must, however, reflect the stage reached in the investigation.

The initial notification phase should allow the controller to state that the assessment of the consequences or risk is ongoing. A detailed analysis of the possible combination of the data with other sources, their future misuse or the ultimate severity of the impact will generally require a separate expert assessment.

Moreover, the wording according to which data were disclosed 'beyond the scope of the privacy policy or relevant legislation' conflates the factual consequences of the incident with a de facto legal assessment of the lawfulness of the processing, which is not the subject matter of a personal data breach notification.

8. **Field 92**

As regards measures intended to address the incident, we reiterate that these measures may not always be known during the initial stage.

9. **Field 94**

The GDPR itself does not require this information, which concerns subsequent prevention. Moreover, such measures often result from a relatively complex process of evaluating the incident and drawing lessons from it. In practice, these measures may therefore be identified and decided upon only weeks after the causes of the incident have been established. It is unclear to us why they should have to be provided where this would necessarily require a further supplementary notification.

10. **Field 99 - future date of communication to data subjects**

We note that, at the time of notifying the supervisory authority, the controller may not be able to determine the specific date on which the breach will be communicated to the data subjects.

11. **Fields 109 to 111 (and 122 and 123) - notifications to other authorities**

Information about reports made to the police, cybersecurity authorities or other regulatory authorities may be useful for coordination among public authorities. However, providing such information should remain optional and should have no bearing on the assessment of compliance with obligations under the GDPR.

At the time the data protection authority is notified, the incident may in any event not yet have been reported to another authority (where the notification to the supervisory authority is made first).

Spolek pro ochranu osobních údajů

12. Field 125 - attachments to the notification

We do not consider the routine attachment of internal documents appropriate. Attachments may contain extensive security-sensitive information, personal data relating to other persons, trade secrets, information on vulnerabilities or communications protected by professional secrecy.

It is also unclear what is meant by a 'dated copy of the risk-assessment'. This could refer to an assessment of the risk arising from the specific incident, a security risk assessment, a DPIA or another internal document. The terminology used in the field should be clarified.

Internal cybersecurity incident investigation reports are particularly sensitive. They may contain preliminary findings, information relevant to criminal or administrative liability, or legal advice. Requiring such reports may also raise issues concerning the privilege against self-incrimination and the protection of confidential communications with legal advisers.

We therefore recommend that all attachments be designated as voluntary.

Prague, 05.08.2026

JUDr. Vladan Rámiš, Ph.D.

Chairman of the Committee
Data Protection Association

JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/E CIPM FIP
Chairman of the Cybersecurity Committee
Data Protection Association