bitkom

Position Paper

August 2026

Bitkom on the EDPB´s Template (2026) for personal data notification

Summary

Bitkom welcomes the initiative of the European Data Protection Board (EDPB) to develop a harmonised template for personal data breach notifications and thereby provide important guidance for controllers and supervisory authorities. However, the current draft, comprising approximately 30 pages and 126 fields, goes significantly beyond the four categories of information explicitly required under Article 33(3) GDPR., namely information on the nature of the personal data breach, the relevant contact point, the likely consequences of the breach, and the measures taken or proposed to address it. Requiring controllers to provide information beyond the categories set out in Article 33(3) GDPR would, in practice, result in a significant additional administrative burden.

At a time when European businesses and policymakers are actively discussing regulatory simplification and the reduction of compliance burdens, it is important that any further development of personal data breach notification requirements remains proportionate and practicable. Bitkom therefore encourages the EDPB to carefully balance effective supervisory oversight with the need to avoid unnecessary administrative burdens for controllers, in line with the broader objective of reducing regulatory complexity and ensuring practical applicability as reflected in the Helsinki Statement.

Bitkom recommends that the EDPB reconsider its current approach, ensuring that the notification requirements are proportionate and appropriate. This would allow all controllers, particularly small and medium-sized enterprises (SMEs), to comply with the requirements in a practical manner. At the same time, the EDPB should clearly demonstrate the practical added value of the additional information requested. A harmonised notification template should improve the efficiency and quality of personal data breach notifications, rather than primarily creating additional administrative obligations for controllers. The following comments outline key concerns and provide practical recommendations for revising the template.

1. Disproportionately Extensive Template

The EDPB template contains almost 100 individual information fields and therefore goes significantly beyond the four categories of information explicitly required under Article 33(3) GDPR. A comparison with existing and established templates used by supervisory authorities in France (CNIL), Spain (AEPD) and Ireland (Data Protection Commission) demonstrates that these templates are considerably more concise and maintain a substantially lower reporting burden.

If the template were to be completed in its entirety for all risk levels, this would create a significant additional burden for organisations in practice. Considering current supervisory authority practices and the typical feedback provided following notifications, the practical added value of requiring such extensive information is not apparent.

Furthermore, notifications must generally be submitted within a very short timeframe (72 hours after becoming aware of the breach pursuant to Article 33 GDPR). Completing such an extensive template would require significant resources that are urgently needed for fact-finding, risk assessment and internal documentation of the incident.

a. Enabling a distinction between initial notifications and follow-up notifications

In the event of a personal data breach, organisations are frequently required to gather information regarding the scope, likely consequences, root cause and other circumstances of the incident within a very limited timeframe. This initial investigation must be conducted promptly in order to comply with the statutory notification deadlines.

In practice, organizations are therefore often forced to provide only approximate details or information at a high level of abstraction in an initial report, for example because not all information is available in a timely manner or because there is not yet sufficient certainty regarding certain facts.

The fact that not all information requested under the draft template can necessarily be provided at the time of the initial notification is also recognised by Article 33(4) GDPR, which expressly permits subsequent supplementation of the notification.

This is particularly relevant for complex IT security incidents, where key information can only be established following forensic analysis. Technical details relating to affected systems, implemented security measures, involved third parties, or the precise risks for data subjects are often unavailable or cannot be reliably confirmed within the 72-hour notification period. Likewise, comprehensive risk assessments and information on the methodology used to assess the breach frequently evolve over the course of the investigation.

Requiring controllers to provide such detailed information already at the stage of the initial notification risks shifting the nature of the notification from an early warning

mechanism towards a nearly complete incident report. This is difficult to reconcile with the objective of Article 33 GDPR, which is intended to ensure that supervisory authorities are informed without undue delay, even where the investigation is still ongoing. An early notification enables supervisory authorities to intervene where appropriate, provide guidance to the controller or require specific remedial measures while the incident is still being investigated.

Furthermore, the level of detail requested is likely to increase internal coordination efforts considerably, particularly in larger organisations where legal, privacy, IT security, forensic and incident response teams all contribute to the notification process. Diverting these resources towards completing an extensive questionnaire during the critical initial response phase may unnecessarily delay incident analysis and containment activities.

The extensive level of detail may also reduce the overall quality of the information provided. During the first days following the discovery of a personal data breach, the factual picture typically develops continuously. As investigations progress, initial assumptions are frequently refined or corrected. Requiring highly detailed information at this early stage therefore increases the likelihood that notifications will subsequently need to be amended, creating additional administrative work for both controllers and supervisory authorities without necessarily improving the usefulness of the initial notification.

Bitkom therefore recommends that the draft template explicitly distinguish between an initial notification (”new notification”) and a supplementary follow-up notification (”follow-up notification”). This distinction is particularly relevant in areas such as sales or customer service, where minor personal data breaches occur on a daily basis and may nevertheless trigger a notification obligation.

For such ”ordinary” risk scenarios (e.g. misdirected shipments), a differentiated approach consisting of a concise initial notification followed by subsequent supplementation would provide a more practical and proportionate solution.

b. Comparison with existing national templates

In Germany, notifications to the competent supervisory authorities are already submitted electronically using templates that request the essential information in a significantly more concise manner (see, for example, the Bavarian State Commissioner for Data Protection (BayLfD): notification of personal data breaches; Bavarian State Office for Data Protection Supervision (BayLDA): reporting a data breach).

Despite the relatively streamlined nature of these forms, completing them following an internal investigation and risk assessment already requires considerable time and resources in practice. Applying the EDPB template to daily, low-risk incidents would therefore create a substantial additional burden for most organisations. Moreover, practical experience shows that, following submitted notifications, supervisory authorities do not always provide feedback, or such feedback often contains only limited substantive comments regarding the incident.

For personal data breaches involving a ”high risk” to individuals’ rights and freedoms, a more extensive questionnaire may be justified. However, for routine practice involving lower-risk incidents, a significantly reduced and risk-based template would be necessary.

2. Level of Technical Detail, Protection of Sensitive Information and Further Recommendations Regarding the EDPB Template

The current draft EDPB template requires a high level of technical detail in several sections and requests the submission of extensive supporting documentation. This significantly increases the reporting burden, particularly for operators of critical infrastructures and SMEs. Furthermore, the structure of the questionnaire may require the disclosure of potentially cyber-sensitive information and business secrets. Without adequate safeguards and recognition of applicable legal privileges, the transmission of such information may create risks to the security interests and commercial interests of reporting organisations.

The following sections therefore identify specific areas of concern and provide practical recommendations for adapting the template.

a. Limiting technical detail and ensuring the protection of sensitive information

Fields 63 and 125 contain extensive requirements regarding technical information. Completing all requested information in these sections may require considerable resources. Notification requirements should therefore remain proportionate and ensure that the required level of technical detail is appropriate for the purpose of the notification.

Furthermore, some of the requested information (e.g., information about ransomware incidents, phishing materials, IT architectures, or forensic reports) may include cyber-sensitive information or business secrets that require special protection. When the transmission of such information is necessary and proportionate, supervisory authorities should provide assurances that the information will be protected and legal privileges respected.

The questionnaire requests detailed information regarding affected systems, software, infrastructure and vulnerabilities. Such information is particularly sensitive for operators of critical infrastructures and could pose security risks if requested or processed at an overly granular level. It should therefore be ensured that security-relevant details only need to be provided at an appropriate level of abstraction.

b. Examples of substantive extensions compared to current practice

The EDPB draft extends beyond current practice in several respects.

- No. 43 et seq.: Ten questions regarding the date and time of the personal data breach and its deletion.
- No. 54 et seq.: A more extensive description of the incident and its effects on confidentiality, integrity, availability and other relevant aspects.
- No. 74 et seq.: Detailed description of all technical and organisational measures (TOMs) in place at the time of the incident (including pseudonymisation measures, access control concepts, etc.). In this context, the specific requirements applicable to critical infrastructures should also be taken into account. The focus should be on whether such measures were implemented rather than on detailed technical descriptions
- No. 96 et seq: Extensive information requirements regarding whether, when and how affected individuals will be informed and whether notifications have been issued.
- No. 124 et seq: Requirement to provide, as annexes, among other documents, communications sent to affected individuals, risk assessments, internal processes and reports relating to the investigation of the incident. By comparison, the current approach of the Bavarian supervisory authority (BayLfD) only requires the submission of the risk assessment.

  If the draft template were adopted by supervisory authorities only in a modular manner, with mandatory fields and required annexes being appropriately limited, the additional administrative burden could potentially be reduced. However, the EDPB indicates that the template is intended to be adopted by supervisory authorities as an online form.

Clarification of the territorial scope of application

Currently, the relationship between the proposed EDPB template and the existing national templates used by supervisory authorities remains unclear. If national templates are ultimately replaced by a final EDPB template, a single-submission approach should be considered. With this approach, a notification submitted to the lead supervisory authority (LSA) would fulfill the requirements of Article 33 of the GDPR for all concerned supervisory authorities.

Severity of potential impacts – need for a reference framework

The proposed Field 87 requires organisations to classify the severity of potential impacts as ”low”, ”medium”, ”high” or ”to be determined”. However, the draft template does not provide any standard or reference framework for this classification.

Without appropriate guidance, there is a risk of significant inconsistencies in the assessment of comparable incidents by different organisations.

Bitkom therefore strongly recommends supplementing the requirements of Field 87 with appropriate guidance, for example based on ENISA recommendations regarding methodologies for assessing the severity of personal data breaches.

Confirmation of accuracy and liability – standard of reasonable knowledge

Field 26 requires the notifying person to confirm the accuracy of all information provided and to assume responsibility for the submitted information. It should be clarified that such responsibility cannot extend beyond the level of knowledge that the organisation could reasonably have obtained at the time of notification (”reasonable knowledge”).

Further recommendations

In addition, Bitkom would like to make the following recommendations

- **Retention period for notification data:** A retention period for notification data should be established that aligns with the data minimization and storage limitation principles under Article 5(1)(c) and (e) of the GDPR.
- **Publication of practical examples:** Completed sample notifications (mock-ups) should be published for both initial notifications and follow-up notifications in order to facilitate practical implementation.
- **Consideration of pending legislative developments:** The planned Digital Omnibus initiative may have implications for certain aspects of the draft template, including the 72-hour notification logic (Field 49) and risk differentiation (Field 89). These aspects should therefore be reviewed, where appropriate, before the template is finalized. In any case, we suggest that the rules and facilitations introduced through the Digital Omnibus should either be awaited or aligned in line with those proposals to avoid divergent regulatory content.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact person

Elena Kouremenou | Policy Officer for Data Protection

P +49 30 27576-425 | e.kouremenou@bitkom.org

Isabelle Stroot | Head of Data Protection Law and Policy

P +49 30 27576-228 | i.stroot@bitkom.org

Responsible Bitkom committee

WG Data Protection