BSA SUBMISSION ON THE EUROPEAN DATA PROTECTION BOARD'S DRAFT TEMPLATE FOR PERSONAL DATA BREACH NOTIFICATION

Response to the Public Consultation

August 5, 2026

The Business Software Alliance (www.bsa.org) welcomes the opportunity to provide input on the European Data Protection Board's (EDPB) draft template for personal data breach notification.

BSA is the global trade association of the enterprise software industry, representing companies[1] that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in more than 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation. BSA's members provide privacy- and security-protective services to business customers across every sector of the economy.

BSA supports the EDPB's efforts to provide clear mechanisms for controllers to report breaches of personal data. At the same time, we are concerned that the draft template is so prescriptive that it will increase confusion for organizations rather than help them prioritize key actions to respond to a data breach.

The detailed and prescriptive draft template creates significant concerns because it goes well beyond the four elements that Article 33 of the General Data Protection Regulation (GDPR) requires a breach notification to include. In this regard, the draft template creates tension with the European Commission's simplification effort, which should be understood not only as clarification of existing rules, but as ensuring that the GDPR framework can be applied in a predictable, scalable, and operational manner. The detailed and prescriptive approach in the draft template is also inconsistent with the effort to promote a streamlined and single route to report incidents. BSA supported the creation of a single-entry point for incident reporting across GDPR, NIS2, DORA, the Cyber Resilience Act (CRA), eIDAS, and the Critical Entities Resilience (CER) Directive, as

---

[1] *BSA's members include: Adobe, Akamai, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systèmes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.*

included in the General Digital Omnibus. The principle of "report once, share many" can significantly reduce administrative burden, improve consistency, and strengthen coordination among competent authorities.

Our recommendations focus on ways that the EDPB can revise the draft template to better align with the GDPR and to create practical tool that companies can use to carry out their notification obligations.

1. The Draft Template's Prescriptive Approach Far Exceeds the GDPR's Requirements

The GDPR sets out four requirements for notification of a personal data breach. Under Article 33, a notification must: (1) describe the nature of the personal data, (2) communicate the name and contact details of the data protection officer or other contact point, (3) describe the likely consequences of the personal data breach, and (4) describe the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects. These notice requirements are high-level and therefore can be adapted to a range of potential scenarios and adopted by a range of different actors.

The draft template goes well beyond GDPR's requirements — with 126 fields, only 10 of which are marked as not mandatory. In contrast, existing templates proposed by DPAs in France, Spain and Ireland are roughly one third the size of the EDPB's draft template.[2]

The level of detail and complexity expected by the EDPB is simply impossible for practitioners to meet within a 72-hour time window. Rather, the draft template's detailed and burdensome requirements will take significant amounts of time for organizations to complete, making the task of notification more complex for organizations rather than creating straightforward and clear rules. Indeed, much of the information sought by the draft template also goes well beyond the information that Article 33 requires be contained in a breach notification. Instead of providing key notification requirements, the draft template reads more like a response to an investigative order related to a data breach, under Articles 56 and 58. Requiring such granular details in an initial notification is unnecessary and unjustified by Article 33. For example:

- Field 53 requires a controller to disclose additional information about the timeline of the breach including the date on which a data processor became aware of the personal data breach. This is not consistent with Article 33(2), which instead requires data processors to notify data controllers without undue delay about a breach but does not require documentation of a precise awareness date. *This language should be removed. If it is retained, it should be revised to focus on the date of notification by the processor to the controller, rather than the date of "awareness" by the processor.*

[2] Commission Nationale de l'Informatique et des Libertés (CNIL), Preparatory Template for Personal Data Breach Notifications, *available at* trame_des_notifications_de_violations_de_donnees_0.odt; Agencia Española de Protección de Datos (AEPD), Personal Data Breach Notification Form, *available at* https://www.aepd.es/documento/formulario-brechas-en.pdf; Data Protection Commission (Ireland), Report a Breach of Personal Data, *available at* https://forms.dataprotection.ie/breach-notification.

- Fields 55-63 seek detailed information about a breach, far beyond the description of the likely consequences and measures taken to address the breach, as required by Article 33. For example, Field 54 requires companies to indicate whether a breach is a confidentiality breach, an integrity breach, or an availability breach; this goes well beyond Article 33 and may distract from the real facts of a breach. Similarly, Field 56 seeks follow up information about confidentiality breaches, Field 58 seeks additional information about integrity breaches, and Field 59 seeks additional information about availability breaches. These constructs do not reflect how companies address breaches in practice. *They should be removed*.

- Fields 75-76 request extensive information regarding security measures in place at the time of the breach, including controls such as multi-factor authentication, encryption, backups, and auditing practices. This is not consistent with Article 33(3)(d) of the GDPR, which focuses on measures taken or proposed to address and mitigate the breach — not a comprehensive inventory of pre-existing safeguards. Requiring disclosure of existing security measures may also effectively require companies to disclose confidential or proprietary information that could actually undermine their security practices, rather than help protect against a breach. Fields 88-90 and 100 ask about the risk that a breach is likely to create to data subjects — while ignoring that the GDPR does not require notification when a breach is unlikely to result in risks to the rights and freedoms of natural persons. For example, the answer options for Field 89 suggest that organizations complete a notification even if harm is unlikely. That is contrary to Article 33's requirements. *These fields should either be removed or revised to align with the GDPR's requirement to describe the likely consequences of the personal data breach*.

- Fields 112-123 address cross-border data transfers, which are not referenced in Article 33. *These fields should be removed*.

The detailed information contemplated by the draft template will require a significant investment of time from companies to complete each notification, particularly because many of the fields add additional complexity and confusion rather than establish clear, workable requirements that facilitate and streamline the notification process. For example, it is not clear from the draft template how organizations should respond to fields for which they are not yet sure of the answer. Other fields create vague requests for information or seek specific information that may be highly sensitive. For example:

- Field 26 is labelled "Accuracy & Responsibility" and refers to a "checkbox: information on the liability for the accuracy of the information provided" — but it is not clear about what information is actually sought by this field. To the extent this field asks the respondent to state that the information provided is accurate, then it should say so clearly and recognize that the respondent should complete the draft template based on his or her reasonable knowledge. *This field should be removed or significantly revised*.

- Field 87 requires organizations to indicate the severity of the potential impact of a breach on data subjects, including whether those potential impacts are minor, moderate, severe, or still to be determined. However, there is no standard or reference framework to assist companies in making this determination. Without such a framework, there are likely to be huge variations in how organizations classify the impacts. *If this field is retained, it should be accompanied by an appropriate guidance framework, such as the ENISA recommendations for a methodology of the assessment of severity of personal data breaches or other established methodologies.*[3]

This detailed and prescriptive approach is inconsistent with broader efforts to simplify EU obligations and to ensure obligations are workable for companies across industry sectors. It also far exceeds the purpose of breach notification, which is to drive appropriate and timely response to breaches (Recital 85). While the draft template provides helpful guidance on elements that controllers should consider when responding to incidents, suggesting that breach notifications must include all information marked as "mandatory" in the draft is unhelpful and misleading — and implies that even fulfilling every requirement of Article 33 is insufficient to comply with GDPR. We recommend the EDPB reconsider the detailed format of the draft template to ensure that notifications are implemented in a reasonable manner so that all organizations, including SMEs, can comply with them.

BSA recommends that the EDPB:

- **Reconsider the level of detail required in the draft template, to ensure it promotes workable and practical notification obligations and does not reach beyond the GDPR's requirements.**
- **Remove fields that go far beyond GDPR requirements, including Fields 55-63, 75-76, 88-90, 100, and 112-123.**
- **Remove or significantly revise confusing fields, including Fields 26 and 87.**

2. The Draft Template Should More Clearly Distinguish Between New and Follow-Up Notifications

The draft template should also be revised to specifically anticipate that companies will file both an initial notification and one or more follow-up notifications.

Although the draft template includes two fields (3-4) indicating whether the notification is a new notification or a follow-up one, there is significant confusion about how the remainder of the draft template is to be applied in each scenario — particularly when an organization does not have all of the relevant facts.

When an organization experiences a data breach, it is often forced to rapidly search for information about the scope, impact, and root cause of the incident. This fact-finding exercise must be carried out quickly, so that the organization can make appropriate notifications within the relevant deadlines. An organization may need to submit an initial notification before it has concluded its fact-finding. As a result, an organization's initial

[3] ENISA, Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches (Dec. 2013), *available at* https://www.enisa.europa.eu/publications/dbn-severity.

notification may necessarily contain high-level information, including when it has either not identified the relevant facts and whether it has identified those facts with the necessary level of certainty. For that reason, it may be impossible for many organizations to provide all of the information envisioned by the draft template in an initial notification.

The GDPR recognizes this in Article 33(4), but the draft template does not. We strongly recommend making it clear in the draft template that organizations may submit both an initial notification and a follow-up to an initial notification. For example, Field 4 currently anticipates that a notification may be complete, incomplete, or a withdrawal. We strongly recommend revising these categories, so that they allow for initial, supplemental, or withdrawal notifications — without suggesting that a notification may be fully "complete" through a single filing.

BSA recommends that the EDPB:

- **Revise the draft template to expressly anticipate that organizations will submit an initial notification (with high-level information) and one or more follow-up notifications and to more broadly allow for the submission of partial responses.**
- **Revise Fields 3-4 to identify filings as "initial" and "supplemental" — not "complete" or "incomplete."**
- **Revise fields that have a specified list of answers to add options for "unsure" or "to be determined," including Field 38.**

3. The Level of Technical Information Required Should Be Reasonable and Should Protect Confidential Data

In addition to seeking highly detailed information that exceeds the scope of Article 33, the draft template also seeks information that may be confidential or sensitive. Not only is it burdensome to provide this information, but some of the data sought contains either trade secrets or cyber-sensitive elements, such as system architecture or forensic reports, that should be safeguarded in order to protect against future breaches. While it may be proportionate to provide this information in connection with a breach notification in exceptional situations, in the ordinary course the draft template should promote the protection of sensitive details and accommodate legal privileges.

Several fields raise this concern, including:

- Field 63 seeks a description of systems, software, services, and infrastructure involved in the personal breach — and where each is located. This information is highly sensitive and is not required by Article 33. *This field should be removed*.

- Field 125 requests dated copies of at least nine different documents, which can provide a roadmap to the data breach and create significant new security risks if accessed by bad actors. These documents should be given significant protection and only sought in exceptional circumstances, rather than invited for each required notification. *This field should be removed*.

- Field 25 asks for an identification number for the reporting person. This is not necessary and creates new privacy risks for individuals who complete the draft template. *This field should be removed*.

BSA recommends that the EDPB:

- **Avoid seeking highly sensitive information in the ordinary course and only request such information in extraordinary circumstances.**
- **Revise the draft template to affirmatively recognize the need for organizations to protect confidential data and trade secrets and to avoid disclosing information that may create new security risks.**
- **Remove from the draft template fields that create risks to privacy, security, and the protection of confidential information, including Fields 63, 125, and 25.**

4. The Geographic Scope Should Be Clarified

The draft template should expressly address how it intersects with existing templates for data breach reporting by national DPAs. If these national DPA templates will be replaced by a final EDPB template, then the draft template should clarify that filing a single notification to the lead supervisory authority satisfies Article 33 for all concerned authorities.

BSA recommends that the EDPB:

- **Address the intersection of the EDPB's draft template with existing national level templates.**
- **Clearly state that filing a single notification to the lead supervisory authority satisfies Article 33 for all concerned authorities.**

5. The EDPB Should Promote Practical Use of the Draft Template

BSA recommends four practical changes to better promote use of the draft template.

First, a sentence should be added at the top of the template to clarify that it is intended to assist controllers in notifying supervisory authorities about personal data breaches, under Article 33 of the GDPR. Although this scope is evident from the context of the draft template, we strongly recommend adding a short and clear sentence stating as much.

Second, the draft template should be revised to focus on information that is known to the controller completing the notification. For example, Field 109 asks whether an incident has been reported to the police/judicial authorities as a criminal offense and Field 110 asks whether an incident has been notified to other supervisory bodies or control bodies under other relevant legislation. These fields should be revised to ask whether the organization completing the notification reported the incident to police/judicial authorities (Field 109) or to other supervisory authorities (Field 110).

Third, in addition to revising the draft template itself, BSA also recommends the EDPB take practical steps that will help organizations to use a revised and streamlined version of the draft template. In particular, we

recommend publishing examples of a completed template. These examples should cover a range of scenarios, including both initial notifications and follow-up notifications.

Finally, the template should be revised to account for ongoing efforts to develop a "report once, share many" framework. BSA has supported the creation of a single-entry point for incident reporting across GDPR, NIS2, DORA, the Cyber Resilience Act, eIDAS, and the Critical Entities Resilience Directive — a principle reflected in the General Digital Omnibus. However, the scope of that single entry point remains unsettled. Member States have sought to preserve direct notification to national authorities, so its final design may diverge from the model this template should be aligned with. Given that uncertainty, finalizing a highly detailed, standalone template now risks entrenching a notification format that will need to be revised once the broader framework is settled. BSA recommends that the EDPB build sufficient flexibility into the draft template — or treat it as explicitly provisional — so that it can be aligned to a single-entry-point architecture that is still in flux.

BSA recommends that the EDPB:

- **Add a clear sentence at the top of the template to expressly state its purpose is to assist controllers in notifying a supervisory authority of a data breach under Article 33 of the GDPR.**
- **Revise Fields 109-110 to focus on whether the organization made additional notifications, rather than focusing on whether any actors made such notifications.**
- **Publish examples of the completed template, including for initial notifications and for subsequent follow-up notifications.**
- **Revise the template to account for the "report once, share many" framework, by either: (1) aligning the draft with the emerging single-entry-point architecture from the outset or (2) treating the current template as provisional, pending that alignment.**

For further information, please contact Thomas Boué,

Vice President and Director General, Policy – EMEA, at thomas@bsa.org.