July 31, 2026

European Data Protection Board

Submitted via web to the EDPB

Re: Public Consultation on the EDPB Template for Personal Data Breach Notification

To the European Data Protection Board:

We appreciate the opportunity to provide feedback on the European Data Protection Board's (EDPB) proposed Template for Personal Data Breach Notification under Article 33 of the General Data Protection Regulation (GDPR).

Epic is a global healthcare technology company working with healthcare organizations across the European Economic Area and in more than a dozen countries worldwide. We provide an integrated software suite to manage clinical care and back-office operations. Our patient portal, MyChart, puts medical records in the hands of patients, enhancing medical literacy, communication, and wellness. Healthcare provider organizations across the European Economic Area rely on Epic's software in connection with over 20,000,000 patient visits each year. These organizations are subject to the GDPR's breach-notification obligations as controllers or processors of personal data, with Epic acting as their processor or subprocessor, respectively.

We work closely with our customers to prevent and respond to personal data breaches, whether caused by malicious cybersecurity attackers, technical equipment failures, or inadvertent human error. These experiences provide us with direct, practical insight into breach-related matters.

We appreciate the opportunity to comment and would welcome the chance to discuss these recommendations further as the EDPB finalizes the template. Thank you for your consideration.

Sincerely,

Harry Freedman
Director, Public Policy

Amanda Reese
Privacy Counsel

Summary of Main Comments

Epic supports the goals the EDPB has articulated for GDPR Article 33, including the protection of patient and consumer data, consistency in breach reporting across Member States, and reduction of administrative burden. However, based on our experiences to date, we are concerned that the proposed Template for Personal Data Breach Notification (the "template") may complicate the achievement of these goals.

As currently drafted, the template includes over 120 fields, of which only ten are optional, creating expectations for providing significant detail in excess of Article 33(3) requirements and presuming a degree of forensic certainty about an incident which is not consistently available following all breaches. It also does not appear to include instructions about whether it is intended for use only with data protection authorities, creating the potential that organizations might use this when issuing required notifications to impacted data subjects.

Recently, IBM reported that the average cost of a breach is $4.99 Million (USD), with healthcare breaches representing the highest-cost industry. Recovering from attacks takes significant time and effort. Of the organizations IBM studied, 42% had not yet fully recovered from cyberattacks that occurred this year and 71% took more than 100 days to recover. Meanwhile, only 4% of organizations completed their recovery within 50 days.[1] Unfortunately, the staff needed to prepare breach reports are typically the same staff needed to mitigate the incident, creating circumstances where reporting burden directly competes with meaningful incident response work.

As proposed, the template places a significant burden upon controllers in the most critical period when a breach occurs. A reduction of required reporting fields would reduce burden and better align the intent of the template with the reality of reporting requirements' burden.

Specific Comments

Align with the Digital Omnibus

Because the pending Digital Omnibus (COM 2025/837) proposes to reduce the scope for mandatory breach reporting under Article 33, we encourage EDPB to revise the template accordingly when the Omnibus proposals are finalized. We further recommend delaying

[1] IBM, "Cost of a Data Breach Report 2026," https://www-api.ibm.com/adobe/assets/urn:aaid:aem:21111142-1251-4369-86fb-57b82f5bb108/original/as/Cost%20of%20a%20Data%20Breach%20Report%202026.pdf

implementation of the revised template until an appropriate time after any updates to Article 33 become effective. This would ensure controllers are not required to adapt to two successive standards and would decrease administrative burden from rule change uncertainty for organizations who enter compliance.

Package clear usage guidance with the template

Clear, accessible guidance on when a breach must and must not be reported, positioned alongside the reporting tool itself, would reduce the risk of over-reporting low- or no-risk incidents, which dilutes the value of the data that supervisory authorities receive. Ensuring organizations correctly understand both their reporting obligations and the template's intended use is especially important for smaller organizations that may not have dedicated compliance resources.

Reduce the size and burden of the initial notification

We recommend the template explicitly distinguish which fields are required for an incomplete notification from those required for a complete submission, as well as reducing required fields to align with what Article 33(3) requires. This reduction would mirror the approach used by the Office of the Australian Information Commissioner (OAIC) template for breach notifications, which collects critical information about breaches in a straightforward and concise manner. The OAIC template is roughly 7 pages long, clearly distinguishes mandatory and optional reporting fields, allows areas of uncertainty to be left unanswered, and reserves OAIC the right to contact organizations for more information if deemed necessary.[2]

Completion of more detailed fields should only be expected as the investigation matures and certainty about a breach has been obtained. Such phasing is practicable and already exists within the current regime: The Belgian Data Protection Authority operates using a similar system, dividing its own national notification portal into an initial submission within 72 hours and a more detailed follow-up within a defined later period, in this case within 21 days.[3] We therefore recommend explicitly communicating what is necessary for an incomplete report, reducing the number of required fields a controller must report, and allowing phased reporting when controllers lack certainty about the breach, moving the template in line with the Belgian Data Protection Authority reporting mechanism.

[2] Office of Australian Information Commissioner, "OAIC Notifiable Breach Form – for training purposes only," https://www.oaic.gov.au/__data/assets/pdf_file/0008/2240/oaic-ndb-form-for-training-purposes-only.pdf

[3] https://www.autoriteprotectiondonnees.be/publications/manuel-d-utilisation-notification-d-une-violation-de-donnees.pdf