5 August 2026

# Comments on the EDPB Template [2026] for personal data breach notification

*by Peter Craddock*

The European Data Protection Board's proposed template for a common data breach notification form is a welcome step towards harmonisation, as the current variations between national forms and the linguistic complications that arise as a result only add to the significant impact that a personal data breach can have on an organisation.

The template in its current form, however, can still be improved to address various shortcomings, some of which stem from current issues not addressed in the template, others of which are new complications specific to the template.

## I. A missed opportunity to prevent over-reporting

Part of the process of examining an incident involves assessing whether the incident meets the definition of a personal data breach – and if so, whether it has to be notified, and to whom.

In this respect, the template's lack of reference to situations where an incident does not have to be reported is a missed opportunity, for various reasons:

- **Omission of exemption guidance**: Question 57 asks whether compromised data was securely encrypted or rendered unintelligible, and Question 89 touches on low-risk scenarios. Yet the template fails to link these fields back to the EDPB's own Guidelines 9/2022 on personal data breach notification under GDPR, which explicitly confirmed that no notification is required when such protective measures remain intact:

  > *"Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms."* (para. 78)

  Helping organisations identify notification exemptions is not a question of avoidance of rules but of better awareness and understanding thereof, to ultimately allow better compliance.

- **Lightening supervisory authority workloads**: Improving awareness of the applicability of notification exemptions is also in the interest of authorities, as it helps avoid over-reporting, namely reporting of incidents that do not meet the relevant threshold. This lowers the workload of already strained and resource-strapped supervisory authorities.

## II. Mismatch between organisations' workflows and regulators' workflows

The template is structured in a manner that appears disconnected from the practical reality of incident management:

- **Fragmented data entry**: While organisations collect incident-related data organically and thematically, the form splits into vastly different sections questions that are intrinsically linked. For instance, questions regarding the nature of an incident (questions 56 [type of confidentiality

breach] and 60 [nature of the incident]) are separated from fields addressing likely consequences and impacts (questions 79 [likely consequences] and 85 [nature of potential impact on the data subject]). This forces the user to move back and forth within the form to ensure consistency, accuracy and completeness.
**Note** that this concern can be addressed by way of user interface features, such as a persistent sidebar with a summary of key elements, to allow the user to rapidly identify options selected in response to earlier questions.

- **Oversimplified risk assessment fields:** The section on the "severity of potential impacts" is oversimplified, to the point that organisations with a mature approach to personal data breach management may struggle to find a level of detail that corresponds to their own reporting methodology.
  This is because the EDPB writes that where different impacts can occur, only the "highest severity" should be indicated. Yet depending on the context of processing, "physical or mental harm" risks may be less severe in practice than a "limitation of rights" consequence, or the opposite may be true. Forcing organisations to tackle severity in general and not at a more granular level may be counterproductive where the organisation is capable of providing a more granular assessment.

## III. Regulatory scope creep beyond Article 33

The template demands a level of granularity that frequently exceeds the statutory requirements of Article 33 GDPR, in a manner that is moreover likely to increase the complexity of reporting:

- **Desirable versus required:** The template lists various fields as "required" despite them not being required under the GDPR. While such fields may be more *desirable* to facilitate supervisory authority workload, the template should only list as "required" the actual, limited data points that the GDPR itself demands.

- **"Under investigation" ignored:** The template leaves little room for organisations to prepare provisional reporting in the case of an ongoing investigation. Fields should only be marked (and function) as mandatory fields where the organisation has indicated that it will submit a full (or additional) notification. For instance, questions 53 (on the timeline and duration of impacts), 62 (explanations regarding root causes) and 63 (systems/software/services/infrastructures involved in the personal data breach) are often unknown or only partially known during the first days following an incident.

- **Excessive document requests**: The precise list of documents to be attached to the form (such as internal risk assessments) also goes beyond the scope of Article 33 GDPR. A consequence of this demand for documents will likely (legitimately) raise the question as to whether non-provision will be misconstrued by a supervisory authority as non-cooperation. Document requests should be aligned with the requirements of the GDPR, and not excessive or unreasonable.

## IV. Technical efficiency and cross-regulatory alignment

The template comes at a time when many organisations have well structured approaches to personal data breach management, sometimes through workflows and tools that are well integrated within an

organisation. Adding this new template on top, with its differences compared to existing approaches, will likely add complexity and inefficiencies to incident reporting.

In this context, to enable the template to work effectively at scale, the EDPB should – alongside the development (and improvement) of the template – require supervisory authorities to support native APIs or browser-side user preferences to pre-fill recurring data points, such as organisation contact details, sector-related fields etc. It should make it easier for organisations to feed their own data into the supervisory authorities' processes, not force new changes to organisations' workflows.

In addition, the limitation of the template to GDPR personal data breach reporting is unfortunate, with a range of other frameworks (such as NIS2 and DORA) covering similar questions. In this respect, the template gives the appearance of an unfinished product.

## V. Practical prototype

To illustrate these usability issues and demonstrate how interface tweaks (such as an integrated sidebar) can mitigate narrative disconnects, a self-contained, browser-based prototype of the proposed template is available online at https://datalaws.net/edpb-breach-notification.html

As it is a self-contained web application capable of running offline, all the code is included in the HTML file, and the EDPB is welcome to draw inspiration from or copy any elements it desires.