Comments on the EDPB Draft Personal Data Breach Notification Template

These comments are submitted in a personal capacity and reflect only the author's views.

On 10 June 2026, the EDPB published its *Draft Personal Data Breach Notification Template* (hereinafter: "Draft") for public consultation. The Draft states that the template is primarily designed to be implemented by data protection authorities through an IT tool, which suggests that it may become a standard, and potentially mandatory, format for breach notifications.

General comments and concerns

1. Administrative burden within the 72-hour deadline

Completing more than 120 rows in a notification template within the 72-hour deadline, and under the pressure usually associated with a personal data breach, is likely to be highly challenging for controllers. In practice, controllers may skip non-mandatory questions; however, because mandatory and non-mandatory questions appear to alternate without a clear structure, there is also a risk that mandatory fields will be missed. This may lead to error messages, additional time spent identifying omissions, or later requests from supervisory authorities to complete the notification.

2. Scope of information required under the GDPR

The GDPR is binding in its entirety and directly applicable. Accordingly, the scope of breach-notification obligations should remain limited to the requirements set out in the GDPR, unless the Regulation expressly authorises supervisory authorities or Member States to impose additional requirements. Articles 33 and 34 GDPR do not appear to provide such authorisation. For that reason, the template should remain within the limits of Article 33(3) GDPR. From this perspective, requesting information under points 5, 7, 10, 11, 14–17, 20–26, 50–53, 63, 93–95, 96–106, and 108–111 of the Draft appears difficult to justify, particularly where such information is treated as mandatory.

- Point 5: The GDPR does not create an obligation to justify the withdrawal of a personal data breach notification. This field should therefore not be mandatory.
- Points 10, 11 and 14–17: While controllers must identify themselves when notifying a breach, mandatory fields such as the "type of identifier" are not expressly required by the GDPR. Other non-mandatory fields appear mainly to serve statistical purposes for supervisory authorities, which may create unnecessary administrative burden for controllers.
- Points 13, 22, 31 and 36: The template asks for the controller's contact details several times: for the controller, the reporting person, the DPO, and the contact point for further information. Under the GDPR, such information appears justified at most twice: the controller's contact details and either the data protection officer or another contact point.
- Points 20–26: The GDPR does not require information about a separate "reporting person" in addition to the DPO, who is the official contact point with the supervisory authority under Article 39(1)(e) GDPR.

- Points 50–53: The GDPR requires a description of the nature of the personal data breach. This does not necessarily include details on how the breach was discovered, who discovered it, or whether an external actor notified the controller.
- Point 63: The GDPR does not require a description of the systems, software, services, infrastructure, or their locations involved in the breach.
- Points 93–95: The GDPR requires a description of measures taken or proposed to address the current breach. It does not clearly require a description of measures intended to prevent similar breaches in the future.
- Points 96–106: The GDPR appears to require only a yes/no indication as to whether the breach was communicated to data subjects. Further details may be relevant in a separate investigation, but not necessarily in the notification itself.
- Points 108–111: Notification of other bodies, other than data protection supervisory authorities, is not foreseen in the GDPR.

3. Information that may be more relevant to later investigations

Several additional points in the Draft may be relevant in the context of a subsequent investigation, but their connection to the immediate notification obligation is less clear. This applies in particular to points 4, 6, 13, 28–31, 32–36, 37–41, 57, 78–87, 88–90, 112–118, and 119–123. While some of this information may relate indirectly to the nature of the breach, the link appears remote.

- Point 6: Requiring the ID of a previously notified breach may be acceptable only if the supervisory authority issues a registration number immediately and automatically after submission. Otherwise, the controller may have to wait for confirmation even when the case could otherwise be closed earlier.
- Point 13: This overlaps with the concerns noted above regarding repeated contact details.
- Points 28–31 and 32–36: Information concerning the DPO or other contact point should be alternative, not cumulative.
- Points 37–41: The involvement of a processor or joint controller may be relevant to the breach, but requiring detailed information for the notification itself does not appear necessary.
- Point 57: This information may be relevant if the breach is communicated to data subjects. However, details concerning such communication should not necessarily form part of the notification to the supervisory authority.
- Points 78–87: A description of likely consequences and potential adverse effects may relate to the nature of the breach, but it may add little to the understanding of the specific incident.
- Points 88–90: These points appear redundant. A breach must be notified if it is likely to result in risk; if no such risk exists, the breach does not need to be notified.

- Points 112–118 and 119–123: These items may be relevant in the context of a later investigation rather than in the initial breach notification.

4. Risk of turning the notification into a preliminary investigation tool

As indicated above, several requested data points do not appear to concern the specific personal data breach itself. Instead, they seem to support a potential investigation by the supervisory authority following the notification. This raises both practical and legal concerns.

- Practical concern: It is unclear how often supervisory authorities initiate investigations following breach notifications. If investigations are relatively rare, imposing additional administrative burden on all controllers may not be proportionate.
- Legal concern: National procedural laws may impose formal and substantive requirements for initiating an investigation. The template could risk circumventing those requirements, including procedural rights available to controllers during an investigation.

5. Risk of delays and incomplete notifications

The large number of questions may increase the number of notifications submitted as "incomplete", particularly where the required information cannot realistically be collected within 72 hours. This may lead to delays for both supervisory authorities and controllers, and may make the notification process less efficient overall.

* * *

In light of the above, it seems that the Draft goes beyond the scope of the GDPR and does not primarily serve the purpose of notifying personal data breaches, but rather to facilitate the subsequent (but only possible) investigative powers of data protection authorities.

Zsolt Bartfai