Insurance Europe Comments on EDPB Template for Data Breach Notifications

Our reference:	COB-DAT-26-040	Date:	05-08-2026
Referring to:			
Related documents:	EDPB Template for Data Breach Notifications		
Contact person:	Danilo Gattullo, Senior Policy Advisor, Conduct of Business	E-mail:	Gattullo@insuranceeurope.eu
Pages:	2	Transparency Register ID	33213703459-54

Insurance Europe welcomes the EDPB's initiative to develop a common template for personal data breach notifications under Article 33 GDPR. A harmonised template has the potential to enhance consistency across supervisory authorities, improve legal certainty for organisations operating across multiple Member States and facilitate more efficient handling of personal data breach notifications.

Insurance Europe supports the EDPB's objective of promoting a more harmonised approach to personal data breach notifications across the EU. To achieve this objective effectively, the final template should strike an appropriate balance between consistency and usability, ensuring that it facilitates compliance without imposing unnecessary administrative burdens on controllers. In particular, the final template should remain proportionate, practical and aligned with the operational realities of incident response.

Against this background, Insurance Europe would like to draw the EDPB's attention to a number of aspects of the proposed template that could be further refined.

Ensuring proportionality and reducing administrative burden

While detailed information can support supervisory authorities' assessment of a breach, the current template appears excessively lengthy and granular in several areas. Insurance Europe encourages the EDPB to review whether all requested information is strictly necessary for the purposes of Article 33 GDPR and to simplify sections that do not materially contribute to the assessment of the incident.

Preserving a staged notification approach

The template should also make it clearer that controllers may submit an initial notification within the 72-hour period based on the information reasonably available at that stage and subsequently provide additional details through follow-up notifications. It should recognise that many breaches – especially cybersecurity incidents and incidents involving processors or third-party service providers – require extensive technical investigation before reliable information becomes available. Further clarification would be beneficial regarding the practical operation of incomplete and follow-up notifications, including whether information already submitted will be pre-populated in subsequent submissions and how controllers should indicate where information remains under investigation.

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

Providing sufficient flexibility

The use of predefined categories can support harmonisation and facilitate consistent reporting. However, the template should retain sufficient flexibility through "Other", "Additional information" and free-text fields to accommodate the wide range of incidents encountered in practice.

Supporting consistency

Insurance Europe recommends including a glossary of key terms and definitions within the template or accompanying guidance. This would help ensure consistent interpretation across sectors and Member States and reduce the risk of divergent reporting practices.

Bulk notifications

Insurance Europe encourages the EDPB to explore whether the template could support the reporting or administration of multiple substantially similar breaches through a streamlined or bulk-reporting approach where appropriate. This could further reduce administrative burden while maintaining effective supervision.

Detailed feedback on the template

Finally, Insurance Europe would like to provide the following feedback on the various parts of the template:

- **Field Nr. 26:** The confirmation regarding the accuracy of the information and the responsibility ("liability") is placed at the end of the address section. It may create the impression that the declaration applies only to the information provided in the address section (up to line 26), rather than to the information contained in the remainder of the notification form. In addition, the reference to the information pursuant to Article 13 of the GDPR is unclear.
- **Field Nr. 14–18:** The information requested in this section is mostly not required for the notification itself or for the assessment of the personal data breach. Considering the size of the template, queries should be limited to what is absolutely necessary. Furthermore, in field 17 an "Other" field is missing for organisations that do not fit into any of the listed classifications.
- **Section 2.1 to 2.4:** This sections request the contact details of up to five different contact persons (fields 13, 22, 31, 36 and 41). The contact details of one competent contact person should be sufficient and would also be more effective for any necessary communication.
- **Field Nr. 57 a)**: In this case, no notification would be required, as protection continues to be ensured (see Guidelines 01/2021, e. g. 5.1, Case No. 10).
- **Field Nr. 62:** Since the template already requests a short description of the nature of the breach, including detection, awareness, cause, measures in place and, where possible, the root cause, it would be useful to provide further guidance on the expected level of detail.
- **Field Nr. 63:** The template requests detailed information on the systems, software, services and infrastructures involved. It should clarify the level of detail expected at the initial notification stage, particularly where the root cause, affected systems, security measures or related documentation are still being investigated or not reasonably available at that time.
- **Fields 72 and 73:** The fields are not immediately clear. Compiling complex data within the reporting deadline entails a significant amount of extra work, which yields only minimal added value.
- **Field Nr. 125:** The categorisation of the documents does not seem feasible since the documents submitted relate to individual cases and do not always fit into specific categories.