Telefónica comments on EDPB Template for Personal Data Breach Notification

EU Transparency Register Number: 52431421-12

31 July 2026

*** Clasificado CORPORATIVO por TELEFÓNICA. *** Classified CORPORATE by TELEFÓNICA.
*** Classificado como CORPORATIVO pela TELEFÓNICA. *** Von TELEFÓNICA als UNTERNEHMENSINTERN eingestuft.

Introductory Comments

Telefónica welcomes the European Data Protection Board's initiative to develop a common template for personal data breach notifications. We strongly support the objective of increasing harmonisation across supervisory authorities, reducing fragmentation within the European Union and providing organisations with a more predictable and consistent notification framework.

Today, organizations like Telefónica, who operates across several Member States are frequently required to deal with different notification forms and different expectations depending on the supervisory authority concerned. A common template therefore represents an important step towards a more coherent application of Articles 33 and 34 GDPR and should ultimately facilitate cooperation between controllers and supervisory authorities.

While supporting this objective, Telefónica believes that the current version of the template could be further improved to better reflect the operational realities surrounding the management of personal data breaches. Therefore, we are pleased to contribute with the following comments, based on Telefónica's long experience in the application of GDPR.

1. The notification should remain mainly focused on the information available within the first 72 hours

Article 33 GDPR establishes a notification obligation within 72 hours precisely because, during the early stages of an incident, organizations rarely possess complete information.

In practice, the priority during those first hours is to contain the incident, preserve evidence, restore affected systems and minimize the impact on individuals. These activities require the full attention of DPO, security, operational and incident response teams.

For this reason, the notification process should avoid requiring controllers to dedicate significant resources to producing extensive documentation while the incident remains under investigation.

Although the template recognizes the possibility of submitting incomplete notifications, the overall structure still appears to assume a level of knowledge that, in many incidents, particularly cyber incidents, will simply not yet exist.

*** Clasificado CORPORATIVO por TELEFÓNICA. *** Classified CORPORATE by TELEFÓNICA.
*** Classificado como CORPORATIVO pela TELEFÓNICA. *** Von TELEFÓNICA als UNTERNEHMENSINTERN eingestuft.

The notification should therefore primarily capture:

- the facts known at the time;
- the preliminary assessment of the risks;
- the commitment to provide additional information as the investigation progresses.

This approach would remain fully aligned with Article 33 GDPR while allowing organizations to focus on limiting harm rather than producing extensive documentation during the most critical phase of the incident response.

2. Towards a more collaborative notification process

Beyond the specific content of the template, Telefónica believes that the notification process itself could evolve towards a more collaborative model between controllers and supervisory authorities.

Rather than viewing the notification as a single static submission, the process could be conceived as an evolving case file, allowing both parties to progressively exchange information throughout the lifecycle of the incident.

Under such a model:

- **controllers** would submit the information available at each stage of the investigation;
- **supervisory authorities** could request additional information only where necessary and according to the evolution of the investigation;
- **subsequent updates** would build upon previous submissions instead of requiring duplication of information;
- **controllers** would be able to prioritise incident containment, remediation activities and the protection of affected individuals during the most critical stages of the response, rather than diverting technical and security resources to preparing extensive documentation;
- **supervisory authorities** would ultimately receive more accurate, complete and reliable information, as notifications would evolve alongside the factual findings of the investigation; and
- **both parties** would benefit from a more efficient, proportionate and collaborative exchange.

This approach would better reflect the practical reality of incident response, where information becomes available progressively as forensic investigations advance.

It would also **reinforce the accountability principle** by promoting continuous dialogue between controllers and supervisory authorities instead of concentrating all reporting obligations within the first 72 hours.

*** Clasificado CORPORATIVO por TELEFÓNICA. *** Classified CORPORATE by TELEFÓNICA.
*** Classificado como CORPORATIVO pela TELEFÓNICA. *** Von TELEFÓNICA als UNTERNEHMENSINTERN eingestuft.

3. Trust, confidentiality and appropriate procedural safeguards

A collaborative breach-notification framework can operate effectively only where there is a **sufficient degree of trust between controllers and supervisory authorities**. To preserve that trust, both the notification template and the surrounding procedure should incorporate appropriate safeguards ensuring that the information submitted is treated confidentially, that any requests for additional information are necessary and proportionate to the purpose of the notification, and that controllers are not required, within the notification process itself, to produce statements or assessments whose primary purpose or effect would be to establish or acknowledge an infringement.

In this context, two legally and functionally distinct processes should be clearly differentiated:

First, the personal data breach notification procedure should be a **cooperative incident-management mechanism** intended to enable the controller to comply promptly and transparently with Article 33 GDPR. Its purpose is to provide the supervisory authority with information that is reasonably available and objectively necessary to understand the nature and potential consequences of the breach, assess the risks to data subjects, and evaluate the measures taken or proposed to address and mitigate the incident.

Second, **any subsequent inspection, investigation or enforcement procedure pursues a different purpose: determining whether an infringement has occurred** and, where appropriate, establishing liability and imposing corrective measures or sanctions. From the moment such a procedure is initiated, it should be clearly identified as such and be subject to the procedural safeguards applicable to enforcement proceedings, the rights of defense, the right to be heard, access to the relevant case file and, where applicable, protection against compelled self-incrimination.

The information supplied in the context of Article 33 notification should not automatically be treated as an admission of liability or as a substitute for the evidence that must be gathered and assessed in a subsequent enforcement procedure.

The **EDPB should therefore clarify the confidentiality regime applicable to breach notifications**, the purposes for which the information supplied may subsequently be used, the limits applicable to requests for additional information, and the procedural safeguards governing any transition from cooperative incident notification to a formal inspection, investigation or enforcement action. Such clarification would promote timely, complete and transparent notifications, while preserving the legitimate procedural rights of controllers.

*** Clasificado CORPORATIVO por TELEFÓNICA. *** Classified CORPORATE by TELEFÓNICA.
*** Classificado como CORPORATIVO pela TELEFÓNICA. *** Von TELEFÓNICA als UNTERNEHMENSINTERN eingestuft.

Conclusion

Telefónica strongly supports the EDPB's objective of creating a harmonized European notification template and believes this initiative represents an important opportunity to improve consistency across supervisory authorities.

Nevertheless, we encourage the EDPB to ensure that the template remains proportionate to the operational realities of personal data breach management. **The initial notification should be designed as a concise first communication, focused on the information reasonably available within the statutory deadline, while allowing the supervisory authority to receive progressively more detailed information through an iterative and collaborative process**.

Such an approach would preserve the objectives of Articles 33 and 34 GDPR, reduce unnecessary administrative burden during incident response and ultimately improve both regulatory oversight and the quality of notifications submitted by controllers.

We hope that Telefónica's experience, as reflected in the comments above, will contribute to EDPB's important ongoing work to develop this harmonized template and support its practical implementation by Data Protection Authorities.

*****

*** Clasificado CORPORATIVO por TELEFÓNICA. *** Classified CORPORATE by TELEFÓNICA.
*** Classificado como CORPORATIVO pela TELEFÓNICA. *** Von TELEFÓNICA als UNTERNEHMENSINTERN eingestuft.



www.telefonica.com

*** Clasificado CORPORATIVO por TELEFÓNICA. *** Classified CORPORATE by TELEFÓNICA.
*** Classificado como CORPORATIVO pela TELEFÓNICA. *** Von TELEFÓNICA als UNTERNEHMENSINTERN eingestuft.