Connect Europe feedback on the EDPB personal data breach notification template

July 2026

Connect Europe[1] welcomes the opportunity to comment on the European Data Protection Board (EDPB) draft template for personal data breach notification. We understand this template is primarily designed to be implemented by Data Protection Authorities (DPAs) via an IT tool and proposes rules to collect certain information from data controllers, including predefined values to help organizations to comply with GDPR obligations to notify personal data breaches to DPAs, while strengthening consistency across the EU.

While Connect Europe companies welcome the proposal to develop a common template, several shortcomings and weaknesses in the current draft will prevent real simplification of notification workflows for organisations handling incidents across multiple EU jurisdictions and will jeopardise more consistent responses, which should be its ultimate goals.

Therefore, we are pleased to contribute with some comments, based on Connect Europe companies' long experience in the application of GDPR, with the aim to improve the final drafting of the template to better reflect operational challenges faced by organisations and DPAs in the management of personal data breaches.

This contribution is structured in two parts. First, it sets out general remarks on the overall framework, including the objectives, scope, and practical implications of the proposed template. Second, it provides more detailed, targeted comments referring to specific questions and sections of the draft template.

[1] Connect Europe is the voice of the leading providers of connectivity networks and services in Europe. Our members are at the forefront of innovation in the telecom and technology ecosystems, connecting over 270 million Europeans with cutting-edge mobile and fixed networks, such as fibre and 5G. They also deliver advanced services, ranging from first-class IT, AI and cybersecurity solutions to entertainment and content. Connect Europe companies drive the digital transformation of the Continent, accounting for more than 70% of total telecom sector investment in Europe. Connect Europe stands for an improved policy and regulatory environment that enables citizens and businesses to benefit from digital connectivity and services.

General comments

Purpose and expected status of the template

In practice, data breach notifications are often submitted to a single national supervisory authority. Organisations may therefore not always need to notify the same incident to several Supervisory Authorities across different Member States. Although in such cases, the practical added value of an harmonised EDPB template may be more limited for a significant number of controllers, Connect Europe acknowledges the positive impact of a common template with a view to a more coherent application of Articles 33 and 34 GDPR by National Supervisory Authorities.

The EDPB should also clarify whether the template is intended as a non-binding common reference structure, or whether supervisory authorities are expected to adopt or align their national notification mechanisms strictly with its proposed structure and content. In practice, EDPB templates might become *de facto* mandatory for organisations and DPAs, even though it is described as "voluntary". Once DPAs align their systems to a given template, controllers will have no real choice. Therefore, **it is of outmost importance that EDPB considers industry experience to reassess its initial proposal, to ensure that the final template is fit-for-purpose and provides real added value for data controllers and DPAs**. Greater clarity on its legal status and on the expected level of convergence would be important.

Operational feasibility and 72-hour notification timeframe

Several concerns arise regarding the stated objective of simplification and time-saving. The template contains a large number of fields and questions (123 questions across seven sections), including requests for information that appear to go beyond the minimum requirements set out in Article 33(3) GDPR. **Filling such template carefully while at the same time dealing with a live data breach is not realistic within the legal timeframe set by GDPR**. Furthermore, a support tool should not add more obligations and new requests for information than those imposed by applicable laws.

In addition, several questions require information that is typically not available within the 72-hour notification timeframe, as it depends on forensic analysis or detailed risk assessments (e.g. exact numbers of affected people per country, the root cause of the breach, and details of security measures in place at the time etc.). In practice, investigations take days or weeks and this kind of information is not available when the first notification is due. Concrete examples include:

- Question 53, on the detailed timeline and duration of impacts on availability, integrity and confidentiality;
- Question 62, requesting granular descriptions of the root causes;

- Question 63, requiring detailed descriptions of the systems, software, services and infrastructures involved, including their location.

Flexibility for phased and incomplete notifications

The draft should clarify whether all questions will be mandatory for controllers once they are applicable under the template, or whether supervisory authorities will allow flexibility depending on the circumstances of the incident.

While the template formally allows for phased notifications, several questions do not appear to allow controllers to clearly indicate that certain elements are still "under investigation" or "to be determined". This may create practical difficulties when complying with the 72-hour deadline.

Indeed, the option to submit an "incomplete notification" does not go far enough. While controllers are allowed to mark a notification as incomplete and add more information later, which is helpful, it is not entirely clear what minimum information is needed in the first submission to avoid being penalised. A landing "safe harbour" should be a clear and simple baseline for initial notifications.

Impact on breach response and incident management

A key operational concern raised by several DPOs across member companies relates to the overall length and complexity of the template. During a personal data breach, organisations must prioritise rapid containment, mitigation and remediation. A highly detailed notification template risks diverting significant resources towards completing extensive reporting requirements, rather than addressing the incident itself. This could ultimately undermine the effectiveness of breach response efforts.

The template may conflict with a planned EU Single reporting portal

The EU's Digital Omnibus, currently being negotiated by co-legislators, proposes a Single Portal where organisations report once and the information is shared with the relevant Authorities. Once this portal is introduced, EDPB template may become redundant or create double reporting. Controllers should not have to adapt their processes twice.

Furthermore, EDBP template does not reduce the burden from other reporting regimes as a single incident can trigger reporting duties under NIS2, DORA, and GDPR at the same time, each with different deadlines. EDPB template adds another layer of friction without addressing those overlapping obligations.

Controllers should not have to "score the seriousness" of the breach under time pressure

The template requires organisations to "rate the severity of the breach" themselves, at the point of notification, with very limited time for comprehensive assessment and information-gathering. Furthermore, these self-assessments could later be used against the controller in an investigation. Clear guidance and safe-harbour criteria are needed before this feature is included.

EDPB template does not account for delays from data processors

Under the GDPR, processors must notify controllers of a personal data breach without undue delay. In practice, however, controllers may not always receive complete information from processors in time to meet notification deadlines. The EDPB template should explicitly recognise such situations and clarify that controllers should not be penalised where they submit notifications promptly based on the information available at the time.

Specific comments

The comments below refer to individual questions and sections of the draft template and provide more detailed feedback where relevant.

- The draft EDPB template seems to expect notification of certain personal data breaches that are not be subject to the notification obligation under Article 33(1) GDPR. It is worth noting that this approach sits uneasily with the ongoing policy discussions surrounding the Digital Omnibus proposal, which aim to raise the notification threshold and focus reporting obligations on incidents presenting a high level of risk. Examples include:
    - **Question 57**: to the question "Was the data unintelligible to anyone who was not authorised to access it or were individuals not identifiable?", the controller can select "Yes and protection is still intact (e.g. data was securely encrypted or otherwise protected)
    - **Question 60** includes a description of nature of incident which do not qualify as high-risk incidents
    - **Question 89**: to the question "outcome of the risk assessment", controllers can select "The personal data breach is **unlikely to result in a risk** to the rights and freedoms of natural persons"
- Some multiple-choice possibilities foreseen in the template seem a bit restrictive. E.g.:
    - **Question 59**: regarding the type of availability breach, there is only an option to choose "temporary availability issue" and "permanent availability issue" or "not determined", but it seems to focus only on availability issues expressed in time and "total unavailability". It does not foresee other possibilities (e.g. partial availability).
    - **Question 110**: regarding the incident notification to other supervisory authorities, "ongoing" and eventually foresee a possibility to indicate for which authority it is in order and for which it is not (in case a company has > 2 supervisory authorities to notify, don't know if that choice exists).
- **Question 49**: the logic defined for this question to appear might not be correct. This question 49 needs to be shown namely in case "date of awareness of breach" +72h < "current time" and not the opposite.

- **Question 60**: regarding the nature of the incident, there is an option to reply "*Abuse of access privileges by employee*". Such case should not be considered as a data breach on the part of the controller, but as unlawful processing by the employee in question.
- **Question 65**: regarding the categories of concerned data subjects, it is not clear what to do in case of overlap (e.g. a telco customer would be a) a customer but also g) a subscriber and h) a user).
- **Questions 72-73**: the notion of "personal data records" is not defined in a clear manner.
- **Question 83**: there is an error in the "logic" defined for this question: it should not be shown in case of "Integrity =1" but in case of "Availability =1".
- **Question 87**: in the Tooltip, the EDPB instructs controllers to select the highest severity of potential impacts on data subjects if multiple potential impacts can occur. It could be useful to allow controllers to select a severity per "nature of the potential impact" indicated in question 85. If not, it might give the impression that all the different impacts have the highest level of severity.
- **Questions 112 to 123**: for cross-border breaches, the EDPB form requires controllers to identify the lead supervisory authority, the affected EEA countries, approximate data subject counts per country, and the other DPAs to be notified. While each requirement may be justified individually, fulfilling them collectively can involve substantial coordination alongside the ongoing incident response process.
- **Question 115**: there might be a mistake in the Tooltip for this question, as it states "Indicate here the countries concerned by the breach" which is different from the list of EEA where the controller has an establishment.