Feedback on the EDPB Draft Template for Personal Data Breach Notification (Version 1.0)

By Diogo Duarte

The European Data Protection Board's initiative to develop a common template for personal data breach notifications under Article 33 GDPR is welcomed. The objective of increasing consistency across supervisory authorities is both necessary and desirable. Organisations operating across multiple jurisdictions continue to face varying notification requirements, structures, and expectations. A common template has the potential to reduce administrative burden, improve the quality of notifications, and facilitate supervisory authorities' assessment of incidents.

The comments below are intended to support that objective. They focus primarily on the treatment of risk, the relationship between data protection and cybersecurity incident management frameworks, and the role of third parties in breach response.

1. The template approaches risk as a static concept rather than a dynamic process

One of the most significant observations relates to the structure adopted for assessing breach impacts and consequences.

Fields 55 to 59 require organisations to classify incidents according to confidentiality, integrity and availability. Subsequently, fields 79 to 84 require consequences to be assessed separately for each category.

While this structure provides clarity and consistency, it may inadvertently encourage a compartmentalised approach to risk assessment that does not fully reflect the reality of modern incidents.

Many contemporary incidents do not affect a single security objective in isolation. Ransomware incidents provide an obvious example. Such incidents frequently involve loss of availability, potential compromise of confidentiality through exfiltration, and integrity concerns where data may have been modified, manipulated, or rendered inaccessible through malicious encryption. In practice, these impacts are interconnected rather than independent.

Furthermore, breach risk often evolves over time. Information initially obtained through a confidentiality breach may subsequently be used to facilitate fraud, identity theft, unauthorised system access, social engineering campaigns, or other forms of manipulation targeting affected individuals. As a result, the consequences of an incident may change significantly after the initial notification and continue to develop over time.

The current structure focuses primarily on identifying the immediate consequences of each category of breach. Consideration should also be given to how risks may develop over time and how one category of compromise may enable future harms associated with another.

For this reason, I would encourage the inclusion of a dedicated field requiring organisations to describe foreseeable secondary or evolving risks arising from the incident. Such a field would better reflect the dynamic nature of personal data breach risk and would provide supervisory authorities with a more complete understanding of potential impacts on data subjects.

2. Greater emphasis should be placed on risk assessment methodology

Field 89 of the data breach notification template requires controllers to indicate the outcome of their risk assessment, while field 90 requests a description of the methodology used and the relevant factors taken into account.

This is a welcome inclusion. However, in its current form, the methodology appears secondary to the outcome itself.

In practice, understanding how an organisation reached a particular conclusion is often as important as the conclusion itself. Two organisations facing materially similar incidents may reach different conclusions regarding risk depending on the assumptions applied, the threat intelligence available, the weight assigned to different factors, and the methodology used to assess likelihood and severity.

Without a structured explanation of those considerations, supervisory authorities may find it difficult to assess whether similar incidents are being evaluated consistently across organisations and sectors.

I would therefore recommend strengthening field 90 and encouraging controllers to explain:

- the factors considered during the assessment;
- the assumptions underpinning likelihood and severity ratings;
- any threat intelligence or forensic evidence relied upon;
- uncertainties that may affect the assessment; and
- the reasons supporting the final risk classification.

Alternatively, the template could explicitly encourage the attachment of the risk assessment documentation itself, rather than treating this primarily as an optional supporting document under field 125.

3. The template could better reflect the full incident response lifecycle

The data breach notification template contains several fields relating to mitigation and remediation measures, particularly fields 92 to 95.

These sections provide useful information regarding actions taken to address the incident and prevent recurrence. However, the structure appears heavily focused on immediate containment and corrective measures.

Modern incident management frameworks generally distinguish between several phases of response, including identification; containment; eradication; recovery; and post-incident monitoring and improvement. The current template does not clearly differentiate between these phases.

This distinction is important because the risk presented by a breach does not necessarily end when the immediate threat has been contained. In many cases, organisations continue monitoring for indicators of compromise, malicious activity, publication of data on criminal forums, attempted credential abuse, identity theft, or other downstream consequences.

For example, where personal data has been exfiltrated, organisations may implement monitoring activities that continue for months after the initial incident. Similarly, threat actors may delay

publication or exploitation of stolen information, meaning that risks to data subjects remain active long after containment measures have been implemented.

I therefore suggest expanding the mitigation section to distinguish between immediate response measures and ongoing monitoring or long-term risk reduction activities.

This would provide supervisory authorities with a more accurate understanding of how organisations are managing risks throughout the entire incident lifecycle.

4. Greater alignment with cybersecurity incident management frameworks would be beneficial

The relationship between data protection incident reporting and broader cybersecurity reporting obligations is becoming increasingly important. Field 110 asks whether the incident has been notified to other supervisory authorities or control bodies under other relevant legislation, including national cybersecurity authorities.

While this is a useful question, it represents the only meaningful point at which the template explicitly recognises the broader regulatory environment. Many organisations subject to the GDPR are also subject to sectoral cybersecurity obligations or to requirements arising under NIS2. These organisations increasingly operate integrated incident response programmes that assess technical, operational, legal, and regulatory consequences simultaneously.

The template would benefit from stronger alignment with concepts commonly used within cybersecurity incident management. This does not require incorporating NIS2 reporting obligations into the GDPR notification process, but rather, it requires recognising that many incidents are assessed through common response structures and methodologies. A stronger alignment would reduce duplication, improve consistency, and facilitate the exchange of information between different regulatory processes.

5. The role of processors and other third parties should be better reflected

Fields 38 to 41 of data breach notification template identify whether processors, joint controllers, or other parties are involved in the incident. While identifying those parties is important, the template does not sufficiently capture their role in incident response and risk mitigation.

In practice, many incidents originate within processor environments or involve processor-managed systems. Furthermore, processors often play a central role in forensic investigations, containment activities, remediation efforts, vulnerability management, system restoration, and ongoing monitoring. The current structure may inadvertently create the impression that mitigation measures are solely implemented by the controller.

A more accurate representation would allow organisations to identify:

- which party implemented specific mitigation measures;
- which party remains responsible for ongoing remediation activities; and
- whether third-party actions materially contributed to reducing the risks faced by data subjects.

Such information would provide supervisory authorities with a more complete understanding of the response effort and the practical allocation of responsibilities following an incident.

Final remarks

The proposed template represents a valuable and necessary step towards harmonisation of personal data breach notifications across the European Union.

The observations above are intended to strengthen that objective by ensuring that the template reflects the realities of modern incident response and risk assessment practices.

In particular, consideration should be given to:

- recognising the dynamic and evolving nature of breach risk;
- strengthening the role of risk assessment methodology;
- distinguishing between different phases of incident response;
- improving alignment with cybersecurity incident management frameworks; and
- better reflecting the contribution of processors and other third parties to mitigation and remediation efforts.

Addressing these points would enhance both the practical utility of the template and the quality of information available to supervisory authorities when assessing personal data breaches.