Contribution to the Public Consultation on the EDPB Template for Personal Data Breach Notification

Author: Mariana Tfeyl, Attorney at Law (Paris Bar) & External Data Protection Officer (DPO) **Date:** July 2026 **Reference:** Public Consultation on the EDPB Template for Personal Data Breach Notification (Version 1.0)

---

1. Introduction and General Assessment

As an Attorney at Law registered with the Paris Bar and an external Data Protection Officer (DPO) with ten years of practical experience in data protection compliance, I welcome the initiative of the European Data Protection Board (EDPB) to harmonize the personal data breach notification process across Member States. The proposed template (Version 1.0) represents a significant step toward legal certainty and operational efficiency for data controllers, particularly for multinational entities navigating fragmented national notification portals.

The conditional logic and predefined values embedded in the template are highly relevant for an IT-based implementation. However, based on my daily practice assisting both SMEs and large enterprises in crisis management during data breaches, I respectfully submit the following observations and recommendations to enhance the template's practical applicability, particularly concerning the intersection of the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act).

2. Intersection with the AI Act: A Missing Dimension

The current template categorizes the nature of incidents (Section 3.2, Field 60) and their causes (Field 61) using traditional cybersecurity paradigms (e.g., hacking, malware, misconfiguration). While accurate, this taxonomy overlooks the emerging reality of data breaches caused by or involving Artificial Intelligence systems.

With the entry into force of the AI Act, data controllers deploying AI systems (especially high-risk AI systems) face dual reporting obligations. Article 73 of the AI Act mandates the reporting of serious incidents to market surveillance authorities within 15 days (or 2 days for widespread infringements) [1]. When a serious incident involving an AI system simultaneously results in a personal data breach (e.g., an AI model inadvertently exfiltrating training data or generating outputs that disclose confidential personal data), the controller must navigate two parallel notification regimes with different deadlines (72 hours under GDPR vs. 15 days under AI Act).

Recommendation 1: I strongly recommend introducing specific predefined values in Section 3.2 (Field 60: Nature of the incident) to explicitly cover AI-related breaches. Suggested additions include: - "Unintended data disclosure generated by an AI system

output" - "Data poisoning or adversarial attack on an AI model" - "Unauthorised access via prompt injection"

Recommendation 2: In Section 6 (Possible other issues), a new field should be added to allow controllers to indicate whether the breach also constitutes a "serious incident" under Article 73 of the AI Act and whether the relevant market surveillance authority has been notified. This would foster cooperation between Data Protection Authorities (DPAs) and AI regulatory bodies, aligning with the spirit of the AI Act.

3. Practical Challenges for SMEs and the 72-Hour Deadline

Section 3.1 addresses the timeline of the breach. Field 49 requires "Reasons for late notification" if the 72-hour deadline is exceeded. In practice, particularly for SMEs lacking sophisticated Security Operations Centers (SOCs), the exact moment of "awareness" (Field 48) is often legally ambiguous. Is awareness triggered when an IT anomaly is detected, or when the anomaly is confirmed to involve personal data?

Furthermore, the template allows for an "Incomplete" notification (Field 4). However, the psychological barrier for SMEs to submit an incomplete form within 72 hours often leads to delayed, albeit complete, notifications.

Recommendation 3: The tooltip for Field 48 ("Date and time of awareness") should explicitly incorporate the EDPB's own guidance (Guidelines 9/2022), clarifying that "awareness" occurs when the controller has a reasonable degree of certainty that a security incident has occurred and that it has compromised personal data [2]. Providing this clarification directly within the IT tool will significantly reduce over-reporting of mere security anomalies and under-reporting of actual breaches.

4. The Role of the External DPO

Section 2.2 (Identity of the reporting person) and Section 2.3 (Name and contact details of the DPO) are well-structured. However, as an external DPO acting for multiple entities, I frequently encounter situations where the reporting person is the external DPO, acting under a specific mandate from the controller.

Recommendation 4: In Field 23 (Function of the reporting person), the option "DPO" should be split into "Internal DPO" and "External DPO / Legal Counsel". This distinction is crucial for DPAs to understand the governance structure of the notifying entity and to direct follow-up inquiries appropriately. An external DPO often requires slightly more time to gather internal technical logs from the controller, a factor DPAs should consider when assessing the completeness of the initial notification.

5. Assessment of Risk to Rights and Freedoms

Section 4.2 requires the assessment of the risk to the rights and freedoms of natural persons. This is arguably the most complex legal determination in the notification process. The template currently leaves this as an open field or relies on the controller's internal methodology.

Recommendation 5: To ensure consistency across the EU, the IT implementation of this template should integrate a standardized, albeit simplified, risk matrix (e.g., combining the severity of the impact with the likelihood of occurrence, as suggested by the ENISA methodology for data breach severity assessment) [3]. Providing a structured framework (e.g., Low, Medium, High risk) with predefined criteria (e.g., volume of data, sensitivity of data, vulnerability of data subjects) would greatly assist controllers, particularly those without dedicated legal departments, in making accurate and objective risk assessments.

6. Conclusion

The EDPB's effort to standardize the breach notification template is highly commendable. By integrating considerations related to Artificial Intelligence and providing clearer guidance on the concept of "awareness" and risk assessment directly within the tool, the EDPB can transform this template from a mere administrative form into a powerful instrument for compliance and legal certainty.

I remain at the disposal of the EDPB Secretariat for any further elaboration on these practical observations.

References

[1] European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Article 73. https://artificialintelligenceact.eu/article/73/

[2] European Data Protection Board. (2023). *Guidelines 9/2022 on personal data breach notification under GDPR*. https://www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_en

[3] European Union Agency for Cybersecurity (ENISA). (2013). *Recommendations for a methodology of the assessment of severity of personal data breaches*. https://www.enisa.europa.eu/publications/dbn-severity

---