KONFEDERACJA LEWIATAN

Warsaw, August 5th, 2026
KL/519/163/ET/2026

Position of Polish Confederation Lewiatan on EDPB consultation on Template for personal data breach notification

1. **Disproportionately lengthy template - high number of information fields**

The number of information fields proposed by the template is very high (close to 100). The information thus required clearly exceeds Art. 33(3)'s four notification requirements.

Moreover, if we look at the existing recommended templates from France, Spain or Ireland, we see that they are about 1/3 the size of the EDPB proposal. In times where the EU industry is complaining about regulatory burdens and policy makers are actively thinking about simplification, it simply does not seem reasonable to increase the length/duration of a data breach notification beyond the existing burdens. We regret to see that the EDPB proposal does not meet with its own Helsinki commitments. We thus recommend the EDPB to rethink the exercise so that it keeps the notifications burden reasonable so that all data subjects, including SME, can comply with them.

2. **Allow for distinction between new / follow-up notifications**

When organizations are confronted with a data breach, they often have to rapidly search for the information regarding scope, impact, root cause, etc. of the incident. This initial fact-finding exercise must happen fast so that notification can be made within the legal deadlines. In those situations, organizations will often see themselves obliged, in a first notification, to keep the information somewhat approximative and high-level, for example because they do not find all data in time, or because they do not have the necessary certainty about, etc. As a result, it will often not be possible for organizations to provide all the data that is required by the draft template in a first notification. This is also recognized in article 33 (4) GDPR.

Therefore, in accordance with that article, we recommend making it clearer in the draft template that organizations can make a distinction between a new notification, and a follow-up submission of an initial notification.

3. **Keep level of technical information reasonable and protect cyber-sensitive data, trade secrets & legal privilege**

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 50 50 860
recepcja@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie
XIII Wydział Gospodarczy

The fields 63 and 125 contain a list of technical data. Providing all the listed information can easily become very burdensome. The obligations should be kept reasonable and proportionate in scope. Moreover, some of these data (e.g. ransomware, phishing material) can contain cyber-sensitive elements or trade secrets (e.g. architecture, forensic reports) that ought to be well-protected. In exceptional situations where the provision of such information would be effectively required and not be disproportionate, the data protection authorities should provide assurances to the organizations that they are able to protect sensitive details and accommodate legal privileges.

4. **Clarify geographical scope**

It is still unclear what the exact relation is between the (proposed) EDPB template and the existing national DPA templates. If/when the national DPA templates will be replaced by a final EDPB template, then nothing seems to prevent a single-submission filing, whereby one notification to the lead SA should satisfy article 33 for all concerned authorities.

5. **Severity of the potential impacts – reference framework**

The proposed field 87 requires organizations to indicate the severity of the potential impacts: minor, moderate, severe, or to be determined. However, there is no standard or reference framework proposed for ranking the severity. Without such framework, however, there may be huge variations in how organizations classify the impacts. We thus strongly recommend to accompany the requirements in field 87 with an appropriate guidance framework, such as the ENISA recommendations for a methodology of the assessment of severity of personal data breaches.

6. **Sub-type of notification – default assumption of completeness**

Field 4 requires controllers to choose between “Complete”, “Incomplete” and “Withdraw”. We suggest replacing this mandatory choice with a default assumption that every notification is treated as complete, unless the controller subsequently submits a follow-up amending or supplementing it.

The current framing is counter-productive: in market practice, controllers - concerned about the administrative burden and reputational impact of a visible “incomplete” filing followed by supplementary submissions - tend to defer notification towards the end of the 72-hour window in order to consolidate all available information into a single filing. This delays the flow of information to supervisory authorities, contrary to the purpose of Article 33 GDPR, which favours early notification even where information remains incomplete (Article 33(4)). A “default complete, follow-up if needed” model would encourage earlier notifications and simplify the form.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 50 50 860
recepcja@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie
XIII Wydział Gospodarczy

7. **Function of the reporting person – role of the DPO**

Field 23 lists the DPO as the first option for the reporting person. We would encourage the EDPB to use this template as an opportunity to take a clear, harmonized position at EU level on whether a DPO can act as the reporting person in a personal data breach notification on behalf of the controller.

This question is currently answered inconsistently across the EEA. Some DPAs accept the DPO as the reporting person, while others (notably the Polish DPA) take the view that this is incompatible with the DPO's supervisory and advisory role under Articles 38–39 GDPR and creates a conflict of interests, as the DPO would be reporting on the fulfilment of an obligation that they are supposed to monitor. As a result, controllers operating across multiple Member States face divergent expectations for exactly the same act, which is difficult to reconcile within a single internal breach-notification procedure.

Given that the EDPB template is intended to standardize breach notifications across the EEA, we consider that the EDPB should decide the issue one way or the other at Union level, rather than leaving it to individual supervisory authorities to reach diverging conclusions.

8. **Accuracy and responsibility checkbox – reasonable knowledge**

Field 26 asks the reporting person to confirm the accuracy and be liable for all information submitted within the form. It should be clarified that such liability cannot go beyond the reasonable knowledge of the organization at the time of notification. We refer in this regard to our comments under section 2.

9. **Additional suggestions:**

We include some final recommendations, such as:

- Specify a retention period for notification data, consistent with minimization and storage-limitation principles.
- Publish some completed mock-up examples of new and follow-up notifications..
- Take account of pending legislation: The Digital Omnibus may impact the template's hard-coded 72-hour logic (Field 49) and risk split (Field 89), which may need revising before adoption.
- Reinforce the Article 33(1) GDPR threshold by introducing, at the outset of the form, a triage question that allows the controller to confirm that an assessment has been carried out and that the breach is unlikely to result in a risk to the rights and freedoms of natural persons; in which case no notification is required and the form is not submitted.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 50 50 860
recepcja@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie
XIII Wydział Gospodarczy

  - This is important because supervisory practice diverges across the EEA: some authorities in practice require notification even of incidents where the controller has documented a well-founded conclusion that the risk did not materialize (for example, where the data was retrieved before misuse or protective measures were confirmed to be intact).
- This practice is inconsistent with Article 33(1), which limits the notification obligation to breaches „likely to result in a risk", and with EDPB Guidelines 9/2022. A clear triage step in the template would:
  - reinforce that Article 33(1) sets a substantive threshold, not a purely procedural default;
  - reduce the volume of notifications that are not required by law and that dilute supervisory attention from genuinely risk-bearing incidents;
  - encourage controllers to conduct and document a proper risk assessment.

Marek Górski
President of the Polish Confederation Lewiatan

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 50 50 860
recepcja@lewiatan.org
www.lewiatan.org

Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie
XIII Wydział Gospodarczy