Submission package to the EDPB as part of the public consultation. It includes:

1. **Cover Letter (Formal Submission)**
2. **Executive Summary**
3. **Full Legal-Technical Argumentation**
4. **Comparative Governance Table**
5. **Annex: Citations to GDPR and EDPB Guidelines**

1. FORMAL SUBMISSION LETTER

Subject: Consultation Response – Draft EDPB Template for Personal Data Breach Notification (2026)

To: European Data Protection Board

From: Katia Bodard, Senior Group Data Protection Officer

Organisation: INFRABEL & TUC RAIL

Date: 05.08.2026

Dear Members of the European Data Protection Board,

I am submitting this response in the context of the public consultation on the *Template for Personal Data Breach Notification (2026)*. I welcome the EDPB's initiative to harmonise breach-notification practices across the Union.

However, I respectfully object to the inclusion of **"DPO" as an option for the "Function of the reporting person" (line 23)**. This inclusion is inconsistent with the GDPR, contradicts EDPB guidance, and risks undermining the independence and integrity of the Data Protection Officer role.

The attached submission provides:

- a detailed legal-technical analysis,
- references to GDPR provisions and EDPB guidelines,
- a comparative governance table demonstrating the risks of the current proposal.

I respectfully request that the EDPB **remove "DPO" as a selectable reporting function**, require the controller to designate **at least one contact point within the controller's organisation** able to provide technical and operational explanations, allow DPO contact details to be provided separately where relevant, and revise the form so

that it distinguishes GDPR-mandatory information from optional or phased follow-up information.

Thank you for considering this contribution.

Sincerely,

Katia Bodard,

Senior Group Data Protection Officer Infrabel & TUC RAIL, katia.bodard@infrabel.be, 0490/52.81.70

2. EXECUTIVE SUMMARY

The draft breach-notification template includes "DPO" as a selectable option for the reporting person. This is **legally incorrect**, **operationally inappropriate**, and **contrary to EDPB guidance**.

Key reasons:

Recommendation: Remove "DPO" from line 23 of the template as a selectable reporting function. The form should require the controller to designate at least one contact point within the controller's organisation who can provide technical and operational explanations about the breach, while allowing the DPO's name and contact details to be provided separately where the controller chooses the DPO as an additional contact point under Article 33(3)(b) GDPR. The form should separately allow the controller to identify an authorised operational reporting person and should distinguish Article 33(3) mandatory information from optional or phased information, support "under investigation" responses, and integrate visible guidance on notification exemptions.

3. FULL LEGAL-TECHNICAL ARGUMENTATION

1. The GDPR assigns breach-notification responsibility exclusively to the controller

Article 33(1) GDPR

"*The controller shall notify the personal data breach…*"

The DPO is not the controller and cannot assume controller obligations. Including the DPO as a reporting person **misrepresents the legal structure** of the GDPR.

1.1. Section 2.3.1 should require a controller contact point, with DPO details provided separately where relevant

Section 2.3.1 of the template appears to make it mandatory to indicate whether a Data Protection Officer has been designated and, where the answer is affirmative, to provide the DPO's name and contact details. Article 33(3)(b) GDPR only requires the notification to include "*the name and contact details of the data protection officer or other contact point where more information can be obtained*". The wording therefore gives the controller a choice: the contact point may be the DPO, but it may also be another appropriate contact point.

For practical and accountability reasons, the template should require at least one contact point within the controller's organisation who can provide technical, factual and operational explanations about the breach. This controller contact point should be distinguished from the DPO. The controller may also provide the DPO's name and contact details, in particular for data-protection advice, supervisory authority interaction or Article 33(3)(b) contact purposes, but identifying the DPO as the contact point should remain optional and should not replace the need for an operational controller contact point.

2. The DPO's independence is incompatible with operational breach notification

EDPB Guidelines on DPOs (WP243 rev.01)

- **Section on Article 38(3) GDPR – Instructions and exercising tasks and duties in an independent manner:** the DPO must perform their tasks independently and must not receive instructions regarding the exercise of those tasks.
- **Section on Article 38(6) GDPR – Conflict of interests:** the controller or processor must ensure that the DPO is not assigned positions or responsibilities that create a conflict of interest, in particular where those responsibilities would lead the DPO to determine purposes and means of processing or compromise independent oversight.
- **Section on Article 39 GDPR – Tasks of the DPO:** the DPO's role is to inform, advise, monitor compliance, advise on DPIAs, cooperate with the supervisory authority and act as contact point, not to assume controller accountability for operational breach notification.

If the DPO is the reporting person, the DPO would move from an advisory and monitoring function into an operational decision-making role. Operational breach notification requires determining whether the breach is notifiable, selecting and validating the facts to be reported, deciding on timing and submitting the notification on behalf of the controller. These are controller responsibilities under Article 33(1) GDPR and not part of the DPO's statutory tasks under Article 39 GDPR.

In practice, this would create an incompatible accumulation of roles, whereby the DPO would be expected to act simultaneously as:

- advisor on breach assessment,
- executor of notification,
- auditor of the same process.

This would undermine the separation between independent advice and operational accountability, and would risk placing the DPO in a position where they later monitor or review a process that they have executed themselves.

3. The breach-notification template requires operational detail the DPO should not own

The template appears to request or facilitate the provision of extensive factual and operational information, including:

- forensic analysis,
- technical incident chronology,
- security measures,
- containment actions.

Such information is typically sourced from IT, Security, Legal, business owners and senior management. For that reason, the template should require at least one controller-side contact point able to explain the technical chronology, forensic findings, containment actions and remedial measures. The DPO may advise on data-protection implications, monitor compliance and act as an additional contact point, but should not be required to own, validate or explain operational breach facts on behalf of the controller.

Listing the DPO as reporting person **misleads organisations** into misusing the DPO as an operational resource.

4. Including the DPO as reporting person exposes DPOs to undue liability

Article 38(3) GDPR

"*The DPO shall not be dismissed or penalised for performing their tasks.*"

If the DPO is the notifier, organisations may:

- shift accountability to the DPO,
- pressure the DPO to delay or avoid notification,

- blame the DPO for regulatory outcomes.

This contradicts the protective intent of Article 38(3).

5. The inclusion risks creating divergent practices across Member States

Some organisations may interpret the template as endorsing DPO-led notification. Others will follow the GDPR strictly.

This creates:

- inconsistent governance models,
- uneven protection of DPO independence,
- regulatory fragmentation.

The EDPB should avoid introducing ambiguity.

6. Best-practice governance models separate advisory and operational roles

Across regulated sectors (finance, healthcare, telecom, public sector), the DPO is:

- an **independent advisor**,
- a **monitoring function**,
- a **contact point**, not an operator.

Incident response and notification are handled by:

- Incident Response Team,
- Legal/Compliance,
- Senior Management.

The template should reflect this by distinguishing the authorised reporting person, the controller-side operational contact point and the DPO or other Article 33(3)(b) contact point.

7. Additional concern: the template should distinguish GDPR-mandatory information from optional or follow-up information

Beyond the specific issue of listing the DPO as a possible reporting person, the draft template appears to raise a broader proportionality and legal-basis concern. A harmonised EU template is welcome and can significantly reduce fragmentation

between national reporting forms, especially in cross-border breach scenarios. However, harmonisation should not result in a de facto expansion of Article 33 GDPR or in a form that makes breach notification more complex than required by the Regulation.

- **Mandatory under the GDPR versus mandatory in the template:** the form should clearly distinguish information required by Article 33(3) GDPR from useful but optional information, follow-up information or information that may be requested later by the supervisory authority.
- **Support for phased notification:** where facts are still being investigated, the form should allow controllers to indicate "under investigation", "not yet known" or "to be provided in a phased update", in line with Article 33(4) GDPR and EDPB Guidelines 9/2022, paragraphs 56–58.
- **Notification exemptions:** the form should visibly guide controllers through the situations where notification may not be required because the breach is unlikely to result in a risk to the rights and freedoms of individuals, as reflected in Article 33(1) GDPR and EDPB Guidelines 9/2022, paragraphs 75–80.
- **Avoidance of over-reporting:** a form that does not clearly present exemptions or phased options may encourage unnecessary notifications, increasing the burden on controllers and supervisory authorities without improving protection of data subjects.
- **Consistency and simplicity:** EU-wide consistency is a legitimate and useful objective, but it should be achieved through a proportionate, practical and legally precise form that remains aligned with the minimum content of Article 33(3) GDPR.

For these reasons, the EDPB should revise the template so that it separates strictly mandatory fields from optional or follow-up fields, supports ongoing investigations and phased notifications, and integrates clear prompts on notification exemptions. This would preserve the benefits of harmonisation while avoiding excessive complexity and unintended over-reporting.

4. COMPARATIVE GOVERNANCE TABLE

Governance Element	**Correct GDPR-Compliant Model**	**Incorrect Model (If DPO Is Reporting Person)**
Who notifies the breach	**Controller** (Art. 33(1))	**DPO**, contrary to GDPR
Nature of responsibility	Operational accountability	Oversight function forced into operations

Governance Element	Correct GDPR-Compliant Model	Incorrect Model (If DPO Is Reporting Person)
DPO's role	Advisory, monitoring, and optional Article 33(3)(b) contact point	Decision-maker and notifier
Conflict of interest risk	Controller prevents conflicts and preserves independence	High (WP243 rev.01, section on Article 38(6) GDPR – Conflict of interests)
Independence	Preserved	Compromised (Art. 38(3))
Operational inputs	Provided by IT/Security/Legal and explained by a controller-side operational contact point	Expected from DPO (incorrect)
Regulatory alignment	Aligned with Articles 33, 38 and 39 GDPR and EDPB Guidelines 9/2022	Misaligned
Organisational risk	Clear accountability	Ambiguous accountability
DPO liability risk	Low	High
EU harmonisation	Consistent	Fragmented
Best-practice alignment	Strong	Weak

5. ANNEX: CITATIONS TO GDPR & EDPB GUIDELINES

GDPR

- **Article 33(1)** – Controller's obligation to notify the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- **Article 33(3)(b)** – Notification must include the name and contact details of the DPO or another contact point where more information can be obtained; the contact point does not necessarily need to be the DPO. In practice, the template should allow DPO details to be provided separately while requiring at least one controller-side contact point able to provide technical and operational explanations.

- **Article 33(4)** – Possibility to provide information in phases without undue further delay.
- **Article 33(5)** – Controller's duty to document all personal data breaches.
- **Article 34** – Communication to data subjects where the breach is likely to result in a high risk.
- **Article 38(3)** – Protection of DPO independence and prohibition on instructions regarding DPO tasks.
- **Article 38(6)** – Controller or processor must ensure that DPO tasks and duties do not result in a conflict of interest.
- **Article 39** – DPO tasks: informing, advising, monitoring, DPIA advice, cooperation with the supervisory authority and contact point role.

EDPB Guidelines on DPOs (WP243 rev.01)

- **Section on Article 38(3) GDPR – Instructions and exercising tasks and duties in an independent manner** – DPO must not receive instructions regarding the exercise of their tasks and must be able to act independently.
- **Section on Article 38(6) GDPR – Conflict of interests** – the controller or processor must ensure that the DPO is not assigned positions or responsibilities that create a conflict of interest, including roles that involve determining purposes and means of processing or compromise independent oversight.
- **Section on Article 39 GDPR – Tasks of the DPO** – DPO tasks are limited to informing, advising, monitoring compliance, advising on DPIAs, cooperating with the supervisory authority and acting as contact point; they do not include operational controller responsibility for breach notification.
- **Section on Article 38(1) GDPR – Involvement of the DPO in all issues relating to the protection of personal data** – DPO involvement means timely consultation and proper participation, not ownership or execution of operational notification duties.

EDPB Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, adopted 28 March 2023

- **Paragraph 1** – any reference to WP29 Guidelines WP250 rev.01 should now be interpreted as a reference to EDPB Guidelines 9/2022.
- **Paragraphs 6–7** – controllers and processors should plan in advance, put in place processes to detect, contain and assess breaches, determine whether notification or communication is necessary, and act in a timely manner; information may be provided in phases.
- **Paragraphs 29–35 and 40** – the controller becomes aware when it has a reasonable degree of certainty that a security incident has led to personal data being compromised; from that point, the controller must notify without undue delay and, where feasible, within 72 hours if Article 33(1) conditions are met.

- **Paragraphs 37–41** – the controller must have internal processes, escalation mechanisms and governance arrangements, including identification of who has operational responsibility for managing and notifying breaches.
- **Paragraph 48** – even where a processor notifies on behalf of a controller under proper authorisation, the legal responsibility to notify remains with the controller.
- **Paragraphs 49–55** – Article 33(3) GDPR sets the minimum information required in the notification, including DPO or other contact point details, likely consequences and measures taken or proposed by the controller; additional information may be useful but should not be confused with the legal minimum. Where the form requests technical or operational explanations, these should be supported by a controller-side operational contact point.
- **Paragraphs 56–60** – phased notification is possible where not all information is available within 72 hours, and controllers may update the supervisory authority if later information changes the initial assessment.
- **Paragraphs 75–80** – notification is not required where the breach is unlikely to result in a risk to the rights and freedoms of natural persons, although the risk may need to be re-evaluated over time.
- **Paragraphs 100–105 and 119** – risk assessment must consider likelihood and severity, the specific circumstances of the breach and, where in doubt, a cautious approach.
- **Paragraphs 121–129** – the controller must document all breaches, the facts, effects, remedial action and reasons for notification or non-notification decisions in order to demonstrate accountability.
- **Paragraphs 130–133** – the DPO has an important advisory, monitoring and contact-point role and should be promptly informed and involved throughout the breach management and notification process; these paragraphs do not transfer operational notification responsibility from the controller to the DPO.