Public Consultation Feedback

EDPB Template [2026] for Personal Data Breach Notification

Version 1.0 - Adopted for Public Consultation on 08 June 2026

Submission type	Individual / practitioner contribution
Sector perspective	Information technology / cross-regional operational support / privacy governance
Date	July 2026
Confidentiality note	This submission is intended as a public consultation response. It does not contain confidential business information or personal data beyond the optional submitter details entered separately in the EDPB web form.

Disclaimer: The observations below are based on operational privacy and compliance experience in business workflows involving logs, tickets, remote support, and cross-regional collaboration. They are offered to improve the usability of the template for controllers, processors, and supervisory authorities.

Executive Summary

The proposed EDPB template is a useful step towards harmonising personal data breach notification across supervisory authorities. It provides a structured approach for collecting core information on the controller, reporting person, nature of the breach, affected data subjects, categories of data, mitigating measures, communication to data subjects, and cross-border elements.

From an operational implementation perspective, the template would benefit from additional fields and guidance that better capture how incidents occur in modern enterprise environments, especially in cross-regional support, remote troubleshooting, cloud collaboration, AI-assisted work, and temporary access scenarios.

This submission focuses on six practical improvements:

1. Add an optional Data Flow section to capture source, transfer path, access mode, storage location, and deletion or containment.
2. Distinguish incident, near miss, and confirmed personal data breach, so that organisations can document contained events without overstating the breach status.
3. Distinguish viewing, temporary remote access, download, export, and persistent storage when assessing disclosure and access.
4. Add remote support, screen sharing, remote troubleshooting sessions, and collaboration tools as explicit incident scenarios.
5. Expand governance and organisational controls, including whitelisting, need-to-know restriction, approval workflow, regional data residency, and temporary access management.
6. Add AI-related processing scenarios, such as upload of personal data to generative AI tools or AI-assisted troubleshooting environments.

These suggestions are intended to improve the template's practical usability and support consistent assessment of complex incidents without creating unnecessary reporting burden.

1. General Comments on the Template

The template is strong in its structure and in the use of predefined values and conditional business logic. This can improve consistency for DPAs and reduce ambiguity for organisations completing breach notifications.

In particular, the template already captures several important dimensions: notification type and follow-up status, controller and reporting person identity, involvement of processors or joint controllers, timeline, detection, nature of the breach, categories and number of data subjects, data categories, likely consequences, mitigation measures, notification to data subjects, other authorities notified, and cross-border processing.

However, many enterprise incidents are not easily understood only through data categories and affected numbers. In practice, the most important questions are often: where did the data originate, how did it move, who accessed it, whether it was only viewed or downloaded, whether it was stored outside the original system, whether access was temporary, and whether the data was deleted or contained.

The template should therefore be enhanced with a stronger operational dimension. This would help supervisory authorities understand not only what data was involved, but how the breach actually occurred and whether the impact was effectively contained.

2. Summary of Proposed Changes

Topic	Proposed change	Expected benefit
Data flow	Add optional fields for source, transfer path, parties, access mode, destination, retention, and deletion/containment.	Better understanding of actual incident scope.
Near miss / contained incident	Allow organisations to indicate that an incident was contained before unauthorised disclosure or access occurred.	Avoids overstating incidents while supporting accountability.
Access mode	Differentiate view-only access, screen sharing, download, export, persistent storage, and onward transfer.	Improves risk assessment and mitigation proportionality.
Remote collaboration	Add remote support, video meeting screen sharing, remote debugging, temporary sessions, and shared collaboration boards.	Reflects common enterprise support workflows.
Governance controls	Add whitelisted access, need-to-know, approval workflow, DTA/DPA or transfer approval, regional data residency, and access expiry.	Better alignment with privacy governance and access management practices.
AI-related incidents	Add generative AI tools, AI-assisted processing, prompt input, model output, and AI tool retention as potential incident contexts.	Makes the template future-proof for AI-enabled work environments.

3. Specific Comments and Recommendations

3.1 Add an Optional Data Flow Section

Relevant template area: Section 3.2 and field 63 on systems, software, services, infrastructures and locations.

The current template asks for the systems, software, services and infrastructures involved and their location. This is useful, but it does not fully capture the path of personal data during the incident. For complex operational incidents, especially those involving support tickets, logs, bug reports, collaboration tools, or remote support, data flow is often essential to understanding the real risk.

Suggested optional fields:

- Source of the personal data: e.g. customer device, production system, support ticket, log platform, email, collaboration tool.
- Transfer path: e.g. user -> customer support -> ticketing system -> engineering -> external processor.
- Parties involved in each step: controller, processor, joint controller, internal department, external vendor.
- Mode of access or transfer: view-only, screen sharing, download, export, email attachment, shared link, API call.
- Final storage location: e.g. EU data centre, local device, shared folder, external SaaS platform.
- Retention or deletion status: whether the data remains, has been deleted, has been contained, or is still under investigation.

Suggested wording:

Add an optional section titled "Operational Data Flow" with the following tooltip: "Where relevant, describe how the personal data moved during the incident, including its source, transfer path, parties involved, type of access, storage location, and deletion or containment measures."

3.2 Distinguish Incident, Near Miss, and Confirmed Personal Data Breach

Relevant template area: Section 1.1 notification type and Section 3.2 nature of the personal data breach.

In large organisations, privacy teams often investigate many potential incidents that are later determined not to be personal data breaches, or that were contained before unauthorised disclosure or access occurred. The template currently focuses on notification of a personal data breach, but it could better support follow-up and withdrawal where the initial assessment changes.

The template already allows incomplete, complete, follow-up, and withdrawal notifications. However, it may be useful to include a clearer status option or tooltip for cases where an incident was contained or where reasonable evidence shows that no unauthorised access or disclosure occurred.

Suggested addition:

- Incident contained before unauthorised access or disclosure occurred.
- Potential incident under assessment; personal data breach not yet confirmed.
- Personal data breach ruled out after investigation, with reasons.

This would encourage accountability and documentation without forcing organisations to frame every security or operational event as a confirmed personal data breach.

3.3 Distinguish View-Only Access, Remote Viewing, Download, Export, and Persistent Storage

Relevant template area: Section 3.2, fields on confidentiality breach and incident nature.

The template includes unauthorised access, exfiltration, disclosure, incorrect permissions, email disclosure, public links and other common scenarios. However, it would be helpful to distinguish more precisely how access occurred.

In modern support operations, a person may view personal data through remote screen sharing or a live troubleshooting session without downloading or storing a copy. This is still a form of access and may be relevant for GDPR assessment, but the risk may differ from download, export, persistent storage, or onward transfer.

Suggested access mode options:

- View-only access within approved system.
- Temporary remote viewing or screen sharing.
- Remote support or troubleshooting session.
- Local download to work device.
- Export to file.
- Email or message attachment.
- Shared link or shared folder.
- Persistent storage outside original system.
- Onward transfer to another party.

This would allow controllers to describe the incident more accurately and allow supervisory authorities to assess proportionality of risk and mitigation.

3.4 Add Remote Support and Collaboration Platforms as Explicit Incident Scenarios

Relevant template area: Field 60, Nature of the incident.

The template contains many useful incident categories, including incorrect access permissions, mail misdelivery, open distribution lists, public links, shared drives, and verbal unauthorised disclosure. It could be strengthened by adding scenarios that are common in cross-regional and hybrid work environments.

Suggested additions to incident categories:

- Unauthorised remote support session or remote troubleshooting access.
- Screen sharing of personal data with unauthorised persons.
- Personal data shared in an internal group chat or temporary collaboration group.
- Personal data uploaded to a shared online project board or collaboration platform.
- Personal data accessed through temporary or emergency access rights that were not removed.
- Personal data exposed through live meeting, recording, or transcript.

These scenarios are increasingly common and may not be adequately captured by traditional categories such as email misdelivery or shared folder access.

3.5 Expand Governance and Organisational Controls

Relevant template area: Sections 3.5, 4.3 and 4.4 on measures in place, mitigation, and prevention.

The template already recognises technical and organisational measures such as training, erasure, incident logs, access levels, MFA, periodic audits, pseudonymisation, and up-to-date IT systems. It would be useful to include more operational governance controls that are frequently used in large organisations.

Suggested governance controls:

- Need-to-know restriction.
- Whitelisted access.
- Temporary access with expiry.
- Access approval workflow.
- Data transfer approval workflow.
- Regional data residency control.
- Segregation of regional data environments.
- Data minimisation workflow.
- Privacy review before collection of logs or bug reports.
- Automated deletion or retention schedule.
- Restriction on local download.
- Screen sharing and meeting-recording restrictions.
- Approved collaboration channel requirement.

These fields would help organisations describe practical controls that are not purely technical but materially affect the likelihood and impact of data breaches.

3.6 Include AI-Related Incident Contexts

Relevant template area: Field 60, Nature of the incident; Section 3.2; Section 4.3 and 4.4.

The increased use of generative AI and AI-assisted tools creates new data handling risks. Employees may upload personal data, logs, bug reports, tickets, meeting notes, or user communications into external AI tools for summarisation, translation, troubleshooting, coding or analysis.

Suggested additions:

- Personal data uploaded to generative AI or AI-assisted tool.
- Personal data included in prompt input.
- Personal data exposed in model output.
- AI tool retained prompts or files beyond the intended processing purpose.
- AI-assisted troubleshooting involved personal data outside approved environment.
- External AI provider involved as processor or other party.

Adding these categories would make the template more future-ready and better aligned with emerging operational risks.

3.7 Clarify Cross-Border Processing and Remote Access

Relevant template area: Section 6.2 on cross-border processing and Section 6.3 on processing at non-EU establishments.

The template appropriately includes questions on cross-border processing and non-EU establishments. However, cross-border operational support increasingly involves remote access rather than physical transfer of files. For example, a non-EEA support engineer may view data stored in an EEA system through approved credentials, or may participate in a live troubleshooting session without receiving a file.

Suggested clarification:

- Whether personal data was accessed remotely from outside the EEA.
- Whether the access was view-only or involved download/export.
- Whether access was approved, logged, time-limited, and restricted by whitelist or role-based access.
- Whether the data remained stored in the EEA or was copied outside the EEA.

This clarification would improve consistency in assessing cross-border incidents where the technical data location and the human access location differ.

3.8 Improve Usability for Operational Teams and SMEs

The template is detailed and suitable for implementation by DPAs through an IT tool. For organisations, especially SMEs or operational teams without dedicated privacy staff, the number of fields may be challenging. Recommended tooltips and examples should therefore use practical language and simple scenarios.

Suggested usability improvements:

- Include examples for common operational incidents, such as email sent to wrong recipient, shared folder misconfiguration, unauthorised remote viewing, and AI tool upload.
- Provide a short explanatory note distinguishing mandatory fields, conditional fields, and optional fields.
- Provide examples of complete and incomplete notifications.
- Provide examples of when to make a follow-up notification and when withdrawal may be appropriate.
- Use plain language in tooltips, avoiding excessive legal terminology.

4. Prioritised Recommendations

If only a limited number of changes can be implemented before final adoption, the following three changes would have the highest practical value:

7. Add an optional Operational Data Flow section.
8. Add access mode options distinguishing remote viewing, view-only access, download, export and persistent storage.
9. Add remote collaboration and AI-assisted processing as explicit incident contexts.

These changes would not significantly increase the burden for simple incidents, because they could be conditional or optional. However, they would materially improve the quality of information for complex incidents.

Annex: Draft Wording for Potential Template Additions

Suggested field / tooltip	Draft wording
Operational Data Flow	Please describe, where relevant, the operational flow of the personal data during the incident, including the source of the data, the transfer path, the parties involved, the type of access or transfer, the final storage location, and whether the data has been deleted or contained.
Access Mode	Please indicate how the personal data was accessed or disclosed: view-only access, remote screen sharing, remote support session, local download, export, email/message attachment, shared link/folder, persistent storage outside the original system, or other.
Contained Incident	Please indicate whether the incident was contained before unauthorised access, disclosure, loss, alteration or destruction occurred, and provide the basis for this assessment.
Remote Support	Please indicate whether the incident involved remote troubleshooting, remote maintenance, screen sharing, live meeting, meeting recording, or temporary access by internal or external support personnel.
Governance Controls	Please indicate whether any of the following controls were in place: need-to-know restriction, whitelisted access, time-limited access, approval workflow, regional data residency control, data minimisation workflow, restriction on local download, or automated deletion.
AI-Related Processing	Please indicate whether personal data was uploaded to or processed by an AI-assisted tool, including generative AI, coding assistant, translation tool, summarisation tool, or troubleshooting tool.

Closing Remark

The EDPB template is a valuable step toward harmonised and structured breach notification. The proposed additions would help the template better reflect real-world operational environments and improve the accuracy, proportionality and usefulness of notifications, especially for complex cross-border, remote support, cloud collaboration and AI-assisted scenarios.