CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 20 7367 3000

cms.law

5 August 2026

Position on the EDPB Template [2026] for Personal Data Breach Notification

CMS Cameron McKenna Nabarro Olswang LLP would like to thank the EDPB for the opportunity to provide comments on the Template [2026] for Personal Data Breach Notification ("**Template**"). We welcome the EDPB's initiative to engage with stakeholders and promote a practical, consistent approach to personal data breach notifications that supports effective accountability and security awareness under existing Member State data protection frameworks. Our response reflects our experience in supporting our clients worldwide in handling personal data breach notifications within existing regulatory frameworks. We remain at the EDPB's disposal should they have any questions.

EXECUTIVE SUMMARY

We support the objective of a practical and consistent data breach notification template that assists data controllers in complying with their notification obligations under Article 33 of the GDPR and facilitates the efficient handling of breach notifications by supervisory authorities. We welcome that the Template covers the key information necessary to assess the nature of the breach, the risks to data subjects, and the measures taken or proposed to address those risks. We suggest that the Template should remain closely aligned with the requirements of the GDPR and be applied in a proportionate and risk-based manner. In particular, it would be helpful to ensure that the Template remains focused on the information necessary for managing and assessing personal data breaches, while avoiding the introduction of additional documentation or reporting expectations beyond the requirements of the GDPR.

Our comments address the following issues:

Field 26 - Accuracy & Responsibility Checkbox: The checkbox may not be necessary because the GDPR already makes the data controller responsible for the notification and its contents.

Field 53 - Disclosure of the Processor's Awareness Date: The GDPR does not require processors to record or disclose their exact awareness date; we therefore propose removing this requirement from the Template.

Field 60(n) - Incorrect Access Permissions: The reference to "cloud storage" is not technology-neutral and may unintentionally imply that cloud environments are inherently less secure; we propose using neutral examples instead.

Field 87 - Severity of Potential Impacts: We propose replacing the Minor/Moderate/Severe classification with the GDPR's own risk thresholds to ensure consistency with Articles 33 and 34.

CMS Cameron McKenna Nabarro Olswang LLP is a limited liability partnership registered in England and Wales with registration number OC310335.
Notice: the company does not accept service by email of court proceedings, other processes or formal notices of any kind without specific prior written agreement.

Field 89 - Outcome of Risk Assessment: The field should be clarified to align with the notification threshold under Article 33(1) GDPR.

Field 90 - Risk Assessment Methodology: Article 33 of the GDPR does not require disclosure of the data controller's assessment methodology; this information can instead be requested by the supervisory authority where necessary.

DETAILED COMMENTS

We provide the following, more detailed comments on specific areas where further clarification would improve the Template's workability and alignment with existing obligations under the GDPR.

1. Accuracy & Responsibility Checkbox (Field 26)

Field 26 requires the reporting person to confirm, via a checkbox, liability for the accuracy of the information provided in the breach notification. However, the GDPR already makes clear in its Article 33 that the obligation to notify a personal data breach to the supervisory authority lies exclusively with the data controller. Introducing a separate "accuracy and responsibility" checkbox merely restates what the GDPR already provides. In addition, it may also risk creating ambiguity: if a data controller declines to tick the box, it could be argued that it has not formally accepted the accuracy liability, opening the door to a dispute on responsibility. A cleaner approach would be to omit the field entirely, relying on the existing legal framework which already places full accountability for the notification on the data controller.

2. Disclosure of The Processor's Awareness Date (Field 53)

Field 53 asks the data controller to provide "the awareness date of the data processor". However, the GDPR does not require the processor to record or disclose its precise date of awareness of a personal data breach. Article 33(2) of the GDPR imposes a single obligation on the data processor: to notify the data controller "*without undue delay after becoming aware of a personal data breach*", but it does not require the data processor to create a formal record of the exact time it became aware of the breach for submission to a supervisory authority. By requesting the data processor's awareness date, the Template appears to introduce a documentation requirement that is not expressly set out in the GDPR. The GDPR's "without undue delay" standard is intentionally flexible and depends on the circumstances of the particular case, recognising that a processor may need a reasonable amount of time to verify that a personal data breach has occurred before notifying the controller. For the reasons set out above, we propose deleting the reference to the "awareness date of the data processor".

3. Incorrect access permissions (e.g. cloud storage, shared folder) (Field 60(n))

Field 60 lists the nature of the personal data breach and includes option "n) Incorrect access permissions (e.g. cloud storage, shared folder)". The GDPR is deliberately technology-neutral. Article 32 requires "*appropriate technical and organisational measures*" without prescribing or prejudicing any particular hosting model. By naming "cloud storage" as the illustrative example of incorrect access permissions, the Template may suggest that cloud-based processing is inherently less secure or more prone to misconfiguration - a presumption unsupported by evidence and contrary to the reality that major cloud providers often exceed the security capabilities of on-premise deployments. Another challenge is that in cloud environments, access permissions are typically managed across multiple responsibility layers - the cloud provider's infrastructure layer and the data controller's application layer. The

example as drafted does not distinguish between these layers, risking attribution of the misconfiguration to the cloud processor when it may in fact have been the data controller's own administrative error within a shared responsibility model. A more appropriate and technology-neutral formulation would be: “Incorrect access permissions (e.g. shared folders, databases, storage systems)” - omitting the specific reference to cloud.

4. Severity of potential impacts - Minor/Moderate/Severe (Field 87)

The GDPR uses a binary threshold: “*likely to result in a risk*” (Article 33(1)) and “*likely to result in a high risk*” (Article 34(1)). The Template introduces a tripartite severity scale (Minor/Moderate/Severe) that does not correspond to the GDPR's own terminology. It is unclear how “Minor” maps to the GDPR's threshold of “*unlikely to result in a risk*” (which would exempt from notification entirely under Article 33(1)), and “Moderate” could be interpreted as either meeting or not meeting the “high risk” threshold of Article 34. We therefore propose replacing the proposed severity scale with the GDPR's own risk thresholds to ensure consistency with Articles 33 and 34 of the GDPR.

5. Outcome of risk assessment (Field 89)

Field 89 lists option (c) twice with different content - once as “unlikely to result in a risk” and once as “additional information is needed”. This may be a drafting error. However, if the breach is “unlikely to result in a risk”, notification was arguably not required at all under Article 33(1), yet the Template seemingly expects notification in that case. We therefore propose correcting this apparent drafting error and clarifying that the Template applies only where the notification threshold under Article 33(1) GDPR has been met.

6. Further description of the risk assessment methodology (Field 90)

Field 90 asks the data controller to “*describe the methodology used and the relevant factors*” of its risk assessment is not required by Article 33 of the GDPR. While Article 33(1) triggers the notification based on risk, it does not oblige the controller to disclose its full assessment methodology in the notification itself. This requirement would blur the line between the breach notification and the actual compliance assessment. We therefore propose omitting this requirement from the Template. Where the information provided in the notification gives rise to questions about the controller's assessment, the supervisory authority can request further information, including the methodology used, in the course of its follow-up enquiries.

CONCLUSION

Overall, our position is that the Template should remain a practical tool to facilitate effective and consistent breach notifications, rather than becoming a more prescriptive reporting mechanism that introduces additional documentation requirements or extends beyond the information necessary under Article 33 of the GDPR. A proportionate Template should focus on enabling data controllers to provide the key information necessary to assess the nature of the breach, the risks to data subjects, and the measures taken to mitigate those risks. We therefore consider it important that the Template is clarified to ensure that it supports timely and effective breach reporting in a workable manner, while remaining aligned with the GDPR’s risk-based approach and flexibility.



Emma Burnett
Partner | CMS Cameron McKenna Nabarro Olswang LLP