

Stadtwerke München GmbH Comments on the EDPB Template for Personal Data Breach Notification (2026)

Transparency register number (EU): 17284292859-45

I. Executive Summary

Stadtwerke München GmbH welcomes the EDPB's objective of promoting a harmonised approach to personal data breach notifications across the EU. A common template can support consistency and legal certainty, provided it remains proportionate, risk-based and workable within the strict 72-hour notification period under Article 33 GDPR.
In its current form, the draft template appears considerably more extensive than the minimum information required under Article 33(3) GDPR and may create a substantial additional burden, particularly for routine low-risk incidents. SWM therefore recommends a modular approach, with mandatory fields and annex requirements limited according to the risk level, the nature of the incident and the information reasonably available at the time of notification.
The template should also distinguish clearly between initial and follow-up notifications and clarify its relationship with existing national notification templates.
Particular care is needed where the template requests information on affected systems, software, infrastructure, vulnerabilities or technical and organisational measures. For operators of critical infrastructure, such information may itself be security-critical. The template should therefore require security-relevant information only at an appropriate level of abstraction.

II. Key comments and recommendations

1. Scope of the template

The 30-page template is highly comprehensive and follows a structure that is understandable from the perspective of supervisory authorities. However, its practical usability will depend heavily on how it is implemented in practice. Compared with the minimum information required for a notification under Article 33(3) GDPR, the draft template requests substantially more information.

If the template had to be **completed in full for all risk levels**, it would create a **considerable additional administrative burden** in practice. At the same time, in light of current supervisory authority practice, the **practical added value of such extensive reporting requirements is not sufficiently clear**. It should also be taken into account that notifications must be submitted within a very short timeframe — **72 hours under Article 33 GDPR** — and that completing an extensive template may divert significant resources from the immediate fact-finding, risk assessment and mitigation of the incident. This is particularly relevant for business areas such as sales or customer service, where minor personal data breaches may occur in day-to-day operations and may already trigger a notification obligation.

The final template should also **clearly distinguish between an initial notification and a supplementary follow-up notification**. In many cases, not all information requested in the draft template can be reliably established within the 72-hour notification period. The initial notification should therefore remain concise and **focused on the information reasonably available at the time of notification**, while additional details can be provided subsequently in accordance with Article 33(4) GDPR.

In Germany, notifications to the competent data protection supervisory authority are submitted electronically via templates that request the essential information in a significantly more concise manner (see, for example, the Bavarian State Commissioner for Data Protection (BayLfD): report a data breach; Bavarian State Office for Data Protection Supervision (BayLDA): notification of personal data breaches). Based on practical experience, completing these forms already requires considerable time and resources once the internal fact-finding and risk assessment have been completed. The final template should **clarify its relationship with existing national notification templates**. If national templates are to be replaced by the EDPB template, a **single-submission approach** should be considered, under which a notification submitted to the competent lead supervisory authority would fulfil the notification requirements vis-à-vis all concerned supervisory authorities. In addition, practical experience shows that supervisory authorities do not always provide feedback following submitted notifications, or that such feedback may contain no, or only limited, substantive comments on the incident.

For personal data breaches involving a "high risk" to the rights and freedoms of natural persons, a more comprehensive form may be appropriate. However, for routine lower-risk incidents — such as misdirected correspondence or comparable cases — applying the full template would create a significant additional burden for most organisations. A **proportionate, risk-based and modular approach** is therefore necessary.

2. Content of the template

a. Substantive tightening of requirements

The following examples illustrate areas in which the EDPB draft appears to go materially beyond current notification practice:

- No. 43 et seq. – The draft requests ten questions on the timing and circumstances of the discovery of the incident.
- No. 54 et seq. – The draft requires a significantly more detailed description of the incident and of its effects on integrity, availability and related aspects.
- No. 74 et seq. – The draft requests information on all technical and organisational measures in place at the time of the incident, including pseudonymisation, access rights and comparable safeguards. For operators of critical infrastructure, it is important that such information is requested **only at an appropriate level of abstraction** and does not require the disclosure of security-critical details. The template should therefore clarify that it primarily asks whether such measures were in place, **rather than requiring detailed descriptions of the underlying security architecture**.
- No. 96 et seq. – The draft requests detailed information on whether, when and through which channels data subjects are informed.
- No. 124 et seq. – The draft requires the notification to data subjects, the risk assessment, as well as internal processes and reports used to investigate the incident, to be attached as annexes. In current practice, the BayLDA generally requires only the risk assessment to be attached.

If the final template were implemented by supervisory authorities in a modular manner, with **mandatory fields and annex requirements limited according to the risk level** and the circumstances of the incident, the additional burden could be reduced. However, the EDPB

draft indicates that the template is intended to be adopted by supervisory authorities as an online form. This underlines the need to ensure **proportionality, flexibility and practical usability** before implementation.
Where the template requires confirmation of the accuracy of the information submitted, it should be clarified that such confirmation can **only relate to the level of knowledge that the controller could reasonably have obtained at the time of notification**. This is particularly important where the factual situation is still developing and certain technical or organisational details can only be confirmed at a later stage.

b. Protection of sensitive data

The questionnaire requires detailed information on affected systems, software, infrastructure, vulnerabilities and related technical aspects. This information is **particularly sensitive for operators of critical infrastructure** and may itself be **security-critical** if requested or further processed at an overly granular level. It should therefore be ensured that security-relevant information only needs to be provided at an **appropriate level of abstraction** and that **adequate safeguards** are in place to protect such information.

c. Alignment with pending legislative developments

In addition, pending legislative developments should be taken into account before the template is finalised. In particular, the **planned Digital Omnibus initiative** may have implications for the 72-hour notification logic and risk differentiation. These aspects should be reviewed and, where appropriate, **aligned with future simplification measures** in order to **avoid divergent regulatory requirements**.