Panasonic truly welcomes the EDPB's efforts to standardize the information provided to Supervisory Authorities (SAs) across the EU in the event of a data breach. We also appreciate the opportunity to offer input during the public consultation. The envisaged standardization is highly valuable, as it will significantly reduce the overhead of adapting to different national SA formats, improve consistency, increase legal certainty, and simplify cross-border breach reporting.

We commend the inclusion of tooltips and business logic, which indicate the intention to make the template user-friendly and to ensure consistency. These features can clarify expected inputs and guide users based on previous answers, potentially reducing errors and incomplete submissions. The availability of multiple examples related to data breach types, the nature of the incident, likely consequences, and potential impact on data subjects is particularly useful. Our experience shows that tick boxes and example-driven inputs are well-received by stakeholders contributing e.g., to our internal breach record and often outperform free-text fields for completeness and clarity.

Explicitly allowing for "incomplete" and "follow-up" notifications reflects the real-world complexity of breaches and the 72-hour reporting window. However, the sheer volume and granularity of mandatory fields may pose challenges in practice. When a breach occurs at a deployed processor, obtaining all requested information on short notice is often especially difficult.

To support the EDPB's efforts, we respectfully offer the following recommendations to improve the template's practicality and proportionality:

1. **Streamline the template**
   - Limit mandatory fields to the requirements set out in Article 33 GDPR. The current template requests extensive technical, forensic, and organizational information that exceeds what Art. 33 GDPR requires.
   - Emphasize identifying the truly critical fields needed for an initial notification versus fields that can reasonably be marked as "to be determined" or updated in a follow-up.
   - Ensure the final template clearly distinguishes between information that must be known within 72 hours and information that requires more time and investigation. This will allow initial reports to be submitted promptly while acknowledging that precise numbers or forensic details may be released later.

2. **Nature, circumstances, and summary of the personal data breach**
   - Precisely pinpointing "Nature of the incident" or "Cause" (e.g., internal vs. external malicious) in the early hours of a complex breach can be extremely difficult. Cybersecurity and forensics teams may not have this clarity within 72 hours making an notification incomplete and requiring substantial follow-ups.
   - Whether the data was unintelligible to anyone not authorised and the type of integrity breach may require deep technical assessment. An initial, non-committal answer will likely be standard, followed by more refined information.
   - Determining the root cause or exact technical exploit within 72 hours of discovery is often impossible. Incident response typically progresses from containment to eradication and then recovery, with root cause analysis occurring later, often over an extended period.

3. **Categories and number of data subjects concerned**
   - Identifying the categories quickly is usually feasible, but obtaining exact numbers of data subjects per category, especially in large and complex breaches, is often impossible within 72 hours. Relying heavily on "approximate number" or "number cannot be determined" will be the norm for initial notifications in large-scale incidents. For pan-European companies, aggregating this data across diverse internal systems for different categories can be particularly challenging during a crisis.
   - The listed categories of concerned data subjects (no. 65) include employees (lit. b), minors (lit. d), and vulnerable individuals such as elderly, refugees, disabled people, and victims (lit. i). Please clarify whether employees and minors are vulnerable individuals in line with Art. 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Working Paper 248 rev. 01, p. 10 and 11) given that they are not explicitly listed as vulnerable data subjects (lit. d) in the proposed template.

4. **Categories and number of personal data records concerned**
   - Differentiating between "number of data subjects" and "number of personal data records" is a crucial distinction and adds complexity. Requiring the "type of record: number of data about each concerned data subject" is technically very demanding. Reporting not just how many data subjects are affected, but also for each data subject, the type and number of records is a significant data aggregation challenge under time pressure. Aggregate figures per-subject breakdowns typically require sophisticated data querying and forensic analysis, which often take days or weeks to complete after a breach.