FINANCE FINLAND

European Data Protection Board

## Finance Finland's response to the European Data Protection Board's Template for Data Breach Notifications

Finance Finland (FFI) welcomes EDPB's initiative to establish a common template for personal data breach notifications and supports the objective of improving consistency across Member States. A harmonised notification template has the potential to facilitate compliance for organisations operating across the EU and contribute to a more consistent supervisory approach. However, harmonisation should not be achieved by expanding the scope of information required for the initial notification beyond what is necessary under Article 33 GDPR. FFI considers it important that the template remains proportionate, practical, sufficiently flexible and aligned with the operational realities of incident response.

Article 33(3) GDPR exhaustively sets out the minimum information that must be included in a personal data breach notification, and FFI considers that this should remain the guiding principle for the common template. The template contains several mandatory fields that extend beyond those requirements by requesting a significant amount of additional information, much of which is designated as mandatory. This is reflected, for example, in requests for detailed descriptions of the methodology used for risk assessments, comprehensive technical information regarding the affected systems and infrastructure, and the full content of communications provided to affected data subjects.

In our view, mandatory information should be limited to what is necessary for the initial notification. Any additional information requested should also have a clear legal basis and may be provided through follow-up notifications or upon request by the supervisory authority. In its current form, the proposed template risks functioning less as a notification tool under Article 33 GDPR and more as a broader information-gathering exercise. FFI therefore encourages EDPB to carefully assess whether all mandatory fields included in the proposed template are necessary for the purpose of the initial notification.

This is particularly important given the practical constraints associated with the 72-hour notification deadline. The proposed template significantly expands the amount of information that controllers are expected to collect and requires considerable internal preparation within that timeframe. This creates the risk that controllers submit preliminary notifications based on incomplete information, which may in turn result in multiple follow-up notifications even in relatively straightforward cases. Consequently, the proposed approach increases the administrative burden for controllers without necessarily improving the protection of data subjects or the effectiveness of supervisory oversight.

The template should also recognise the practical realities of personal data breach investigations. Controllers are frequently required to submit a notification while investigations are still ongoing and not all relevant facts are yet available. The template should therefore support a streamlined initial notification, allowing additional information to be supplemented as it becomes available or where requested by the supervisory authority.

Finally, the template should take into account that some of the information requested may be commercially confidential or security sensitive. Detailed descriptions of systems, infrastructures, investigation reports and other technical documentation may reveal confidential business information

FINANCE FINLAND

or expose an organisation's security posture. Such information should therefore not be required as part of the initial notification and should only be provided where it is necessary for the supervisory authority's assessment or specifically requested.

The comments below identify the specific fields where FFI considers that the proposed template could be further aligned with the objectives and requirements of GDPR.

**Specific comments**

Field 25 – National identification number: FFI proposes removing this field. The template should adhere to the principle of data minimisation by avoiding the collection of unnecessary personal data relating to the individual submitting the notification. The identification of the controller and relevant contact details should generally be sufficient for the purposes of the notification.

Field 50 – How was the personal data breach discovered?: The terminology used in the field should be made more consistent. In particular, the terms "communication" and "notification" appear to be used inconsistently, which may create ambiguity for controllers completing the template.

Field 63 – Description of the systems, software, services and infrastructures involved in the personal data breach: FFI considers that requiring controllers to provide detailed technical information regarding the affected systems and infrastructure goes beyond the information necessary to comply with Article 33 GDPR and imposes a disproportionate administrative burden on controllers. In addition, such information may contain confidential business information or security-sensitive details.

Field 69 – Categories and number of personal data records concerned: Special categories of personal data within the meaning of Article 9 GDPR should be more clearly distinguished in the template, given their particular relevance for assessing the potential impact of a personal data breach.

Field 73 – Number of personal data records concerned by the personal data breach: The purpose of this requirement is unclear, and the instructions relating to the "number of personal data records concerned" could be further clarified from a practical implementation perspective.

Field 89 – Outcome of the risk assessment carried out by the controller: The purpose of this option is unclear. Under Article 33(1) GDPR, controllers are not required to notify personal data breaches that are unlikely to result in a risk to the rights and freedoms of natural persons.

Field 90 – Further description of the risk assessment carried out by the controller: The proposed field requires controllers to describe the methodology used to assess the risks arising from the personal data breach, which exceeds the information required under Article 33(3)(c) GDPR. The template should focus on the outcome of the assessment rather than requiring a description of the underlying methodology. Where further explanation is necessary, it should be requested separately by the supervisory authority.

Field 93 – Measures taken (or proposed to be taken): The template should recognise that, at the time of the initial notification, controllers may still be investigating the incident and future mitigation measures may not yet have been identified. Information relating to planned measures should therefore not constitute a mandatory element of the initial notification but should instead be capable of being supplemented through follow-up notifications.

Field 106 – Content of the information provided to data subjects: The GDPR requires controllers to provide certain information to affected data subjects where Article 34 GDPR applies. However, FFI

does not consider it necessary to require the full content of that communication as a mandatory part of the initial breach notification. Such information should only be requested where relevant for the supervisory authority's assessment.

Field 109 – Notification to police or judicial authorities: FFI notes that information regarding whether the incident has been reported to the police or judicial authorities does not form part of the notification requirements under GDPR. The relevance of this field should therefore be reconsidered.

FINANCE FINLAND

Hannu Ijäs