VILNIAUS 31
01402 VILNIUS
LITHUANIA

T +370 5231 2211
E INFO@TRINITIJUREX.LT
WWW.TRINITIJUREX.LT

E.DELIVERY BOX
ADDRESS
302633203

TRINITI JUREX
TALLINN RIGA VILNIUS

To the European Data Protection Board

REGARDING THE COMMENTS ON THE TEMPLATE FOR PERSONAL DATA BREACH NOTIFICATION

Vilnius, 4 August 2026

Following the publication by the European Data Protection Board of the draft Template for Personal Data Breach Notification for public consultation (hereinafter referred to as the Template), we would like to express our support for the objective of harmonising personal data breach notifications across the European Union and providing a common structure for supervisory authorities. We believe that a common template has the potential to improve consistency, legal certainty and the efficiency of supervisory cooperation.

At the same time, based on our practical experience advising organisations of different sizes on Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the GDPR) compliance, including the management of personal data breaches, we would like to submit the following observations and recommendations for consideration. Particular attention is given to the practical implementation of the proposed template by small and medium-sized enterprises (SMEs), as well as to its interaction with other EU cybersecurity reporting obligations. Please find our observations below.

1. THE PROPOSED TEMPLATE EXCEEDS THE MINIMUM INFORMATION REQUIRED UNDER ARTICLE 33(3) GDPR

While additional fields may aid complex investigations, requiring extensive details in the initial notification could delay timely reporting. Article 33 of the GDPR recognises that not all information is available within 72 hours and permits phased submissions; for example, paragraph 63 of the Template requires to specify the systems, software, services and infrastructures involved in the personal data breach and where they are located: from practical perspective, obtaining all relevant information within the implemented 72 hours period is highly challenging and, in many cases, virtually impossible. The template should more clearly separate information needed for the initial notification from that appropriate for follow-up reports.

2. THE TEMPLATE'S COMPLEXITY CREATES A DISPROPORTIONATE BURDEN

With more than 100 conditional fields, detailed taxonomies, and extensive classifications, the template may be difficult to complete without specialised legal and technical expertise. This may discourage timely reporting or not reporting at all, particularly for SMEs that often lack dedicated privacy or cybersecurity teams. A more proportionate approach would be to provide a simplified initial notification and reserve detailed technical information for subsequent reports where necessary.

3. OPTIONAL VERSUS MANDATORY INFORMATION

Information such as detailed root cause analysis, technical system descriptions, extensive mitigation measures, and comprehensive incident timelines may assist supervisory authorities, but it should generally remain optional unless specifically relevant to the circumstances of the breach.

Moreover, paragraph 20 requires to provide personal data of the reporting person such as function, national identification number, which, in our view, the requirement to provide such information is disproportionate to the objective pursued, as it would not provide the supervisory authority with any meaningful added value when assessing the circumstances of the personal data breach or its potential impact. We therefore suggest that the EDPB remove this requirement and retain only the obligation to provide the name and contact details of a person who can provide the supervisory authority with any additional information required in relation to the breach.

4. THE INTERACTION WITH THE NIS2 DIRECTIVE AND NATIONAL CYBERSECURITY LEGISLATION

In many cases, the same event constitutes both a personal data breach under the GDPR and a significant cybersecurity incident under the NIS2 Directive[1]. The proposed template does not sufficiently reflect the „once-only“ principle promoted by EU digital policy, forcing controllers to report substantially identical technical information to different authorities in different formats. We recommend greater interoperability between GDPR and NIS2 reporting frameworks, including the reuse of common incident data.

5. THE LEVEL OF DETAIL IN TECHNICAL CLASSIFICATIONS IS EXCESSIVE

Several technical classifications (for example, detailed incident types, root causes and protective measures) appear better suited to mature cybersecurity incident response teams than to the average controller. Consideration could be given to allowing higher-level descriptions where detailed forensic information is not yet available.

6. A RISK-BASED APPROACH IS NEEDED

We would suggest adopting a clearer risk-based structure throughout the template. The amount of information expected from controllers should be proportionate to the nature, severity and complexity of the breach. Minor incidents affecting a limited number of data subjects should not require the same level of detail as sophisticated cyberattacks involving large-scale processing or cross-border impacts.

Best regards,

TRINITI JUREX

Lithuania

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (hereinafter referred to as NIS 2)