GattiPavesiBianchiLudovici

TMT, INTELLECTUAL PROPERTY AND DATA PROTECTION

Second batch of regulatory and implementing technical standards for DORA

Regulation (EU) 2022/2554, (so called "DORA" Digital Operational Resilience Act), will come into force in January 2025 e aims to create a safer European financial sector by harmonizing and improving the way European financial entities manage their digital operational resilience.
On July 17, 2024, EBA, EIOPA and ESMA, the three European Supervisory Authorities ("ESAs"), released the second round of final reports related to the implementation of DORA.

The documents published on July 17

Specifically, the published documents provide more details on threat-led penetration testing, the design of the oversight framework, the joint examination team that will carry out vigilance tasks, how to estimate costs and losses related to incidents, and the regulatory technical standards for format, content and deadlines of major incident notification.
The technical standards have been submitted to the European Commission and will be finalized in the next months.
The second set of regulatory products does not, as hoped, contain guidelines on subcontracting, still leaving uncertainty about a key element of compliance.

The standards for incident reporting

Document "JC 2024 33" is of pivotal importance for operators, as it outlines regulatory technical standards (RTS) for **content, format, deadlines and procedures for incident reporting, with a**

focus on the need for proportionality and alignment with other regulations such as the NIS2 directive.
Indeed, clarity on the template and how to report will enable operators to build internal reporting procedures more efficiently, creating scalable approaches suitable for focusing compliance efforts against different regulations (e.g., GDPR).

Below are some of the most important elements that emerge from the regulatory technical standards.

Single Template: Under the DORA Regulations, information on significant cyber incidents is to be provided in three stages (**Initial Notification**, **Intermediate Report**, and **Final Report**) To simplify this process and ensure the quality of the data collected, a single template covering the entire cycle of incident reporting has been drafted. The template aims to collect in a single point all the information necessary for the competent authorities to assess the incident comprehensively. Financial entities are required to fill in only the fields relevant to the specific reporting stage being conducted (initial, intermediate, final). While the template is divided into specific sections for each stage, it offers a degree of flexibility. If a financial entity already has information required at a later stage, it can anticipate and fill it out in the template, thus simplifying the reporting process.

Recurring Incidents The template is also designed to handle reports of multiple or recurring incidents that, if taken individually, would not meet the criteria to be classified as a "major incident," despite cumulatively, meeting the threshold for notification. Specifically, recurring incident are non-major incidents that have occurred at least twice within a six-month period, share the same apparent root cause, and collectively qualify as a major incident. The standards provide that information on recurring incidents shall be provided in the final report to address concerns raised by financial entities during public consultation regarding the difficulty of providing a complete root cause analysis at such an early stage in the reporting process and the burden of having to classify and register all minor incidents to determine whether the reporting thresholds are met.

Aggregate notifications: Aggregate reporting is provided in cases where multiple financial entities experience a major IT incident due to a third-party ICT service provider. The specification on aggregate incidents complements the discipline of outsourcing of reporting obligations. In such cases, the third-party provider may submit a single aggregate report for all affected financial entities, provided that specific conditions are met.

Reporting template content: The reporting template has been simplified by significantly reducing the number of fields from 84 to 59, specifically by reducing the initial reporting template to 7 mandatory fields. This change addresses concerns expressed during the public consultation regarding the reporting burden, especially in the early stages of incident management.

Reporting timelines: Many respondents felt that the initially proposed timelines were too short, particularly regarding the intermediate report. As a result, the ESAs decided to extend the timeframe for submission of the intermediate report to 72 hours from the time of the submission of the previous notification, rather than from the time of incident classification. In addition, the standards clarify the possibility of submitting the interim report without undue delay once business as usual has been recovered. As for the final report, the deadline will be one month from the submission of the latest update of intermediate report, removing the reference to the "permanent" resolution of the incident.

Weekend reporting: To ensure a more proportionate approach, ESAs have exempted smaller financial entities from the weekend reporting requirement unless the incident has a systemic or cross-border impact. eliminating the need for all financial entities to have a 24/7 incident reporting support function.

***

We remain available for any further information and to provide all necessary support in order to comply, on time, with the relevant regulatory framework.

GATTI PAVESI BIANCHI LUDOVICI

TMT, Intellectual Property and Data Protection

Gilberto Nava gilberto.nava@gpblex.it

Elisabetta Nunziante elisabetta.nunziante@gpblex.it