Legance

Newsletter

MARCH 2025

News on the reporting of major ICT-related incidents and cyber threats in the insurance sector

Insurance

On 14 February 2025, IVASS published the Letter to the Market (the '**Letter**') setting out operational provisions under EU Regulation 2022/2054 (the 'DORA' – Digital Operational Resilience Act) regarding the reporting of major ICT-related incidents and cyber threats.

The addressees of the Letter are insurance intermediaries[1] as well as insurance and reinsurance undertakings with registered offices in Italy[2].

The DORA, in force since 17 January 2025, is a key pillar for ensuring digital operational resilience in the European financial sector, *i.e.* the financial entity's ability to build, secure and review its operational integrity and reliability to ensure the security of the networked IT systems used by the financial entity[3], including insurance companies. As such, the DORA aims to standardize and strengthen IT and technology risk management in the financial sector focusing on prevention and recovery in the event of cyber incidents.

In the context of the aforementioned regulatory framework, and under the obligations already applicable since last January, the Letter recalls the relevant legislation, thus providing operators with a useful tool to properly comply with the reporting of major incidents, given that the DORA itself (see Article 19) requires financial entities to report serious ICT-related incidents to the competent authorities and to notify, on a voluntary basis, significant cyber threats.

Specifically, the Letter refers to major incidents subject to reporting as defined in EU Delegated Regulation 2024/1772 (see Article 8).

The Letter further aims to specify the timing that financial entities must respect in the event of a major ICT-related incident, since the deadlines for reporting incidents must follow a consistent approach for all types of financial entities. In particular, the reporting steps are divided as follows:

- an initial report, no later than 24 hours after the identification of the incident;
- an interim report, within 72 hours from the initial report with the possibility of sending subsequent updates;
- a final report, within one month from sending the last update of the interim report.

Clearly, the content of these notifications varies depending on the stage of the incident. Indeed, according to EU Delegated Regulation 2025/301 the initial notification should be limited to significant information only. After the initial notification, the competent authorities should receive more detailed information on the ICT-related incident through the interim report and all relevant information through the final report in order to enable the competent authorities to further examine the incident[4].

Finally, the Letter draws attention to the voluntary reporting of cyber threats deemed significant to the financial system[5], service users or customers. Significant cyber threats should only be notified on a voluntary basis, so the content of such notifications cannot be a burden on financial entities, which will certainly have to cooperate with the competent authorities, although with a more limited frequency than the information required for major ICT-related incidents.

The introduction of cyber incident reporting obligations and procedures for voluntary reporting of significant cyber threats requires adequate organisational preparation by the addressees of the Letter. Proactive cooperation is also required to ensure effective coordination in digital crisis management with IVASS[6], it being understood that under the DORA financial entities may outsource reporting obligations to a third party service provider[7].

The attention of the competent authorities is high and considering that there has been no transition period, the supervisory authorities stress the importance of financial entities adopting a solid and structured approach in order to fulfil their obligations in a timely manner. Accordingly, financial entities are required to identify and promptly address internal deficiencies and the obligations set forth under DORA also in light of the provisions of Legislative Decree no. 23/2025[8] concerning the adaptation of national legislation to DORA. Among the updates, it is worth mentioning the amendments to the Insurance Act regarding the sanctions that are applicable in case of non-compliance with specific provisions under DORA, including the failure to report major ICT-related incidents[9].

[1] In this regard, it should be noted that insurance, reinsurance and ancillary insurance intermediaries with more than 250 employees and an annual turnover of more than EUR 50 million or an annual balance sheet of more than EUR 43 million are subject to DORA.

[2] The addressees of the letter also include branches of insurance undertakings with their head office in a state outside the e.e.a.

[3] See Article 2 of the DORA. Financial entities include, *inter alia*, credit institutions, payment institutions, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries.

[4] Templates for complying with the obligation to report major ICT-related incidents and significant cyber threats are attached to the Letter. Reports should be sent to IVASS via certified mail to the following addresses: vigilanza.prudenziale@pec.ivass.it by insurance undertakings; and vigilanzacondottamercato@pec.ivass.it by insurance, reinsurance and ancillary insurance intermediaries.

[5] Article 18 of the DORA specifies that financial entities classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's operations, the number and/or significance of affected customers or financial counterparties, and the geographic extent of the risk areas.

[6] Pursuant to Legislative Decree no. 23/2005, IVASS is the national competent authority to receive reports of major ICT-related incidents and voluntary notifications relating to cyber threats.

[7] See Article 19(5) of the DORA Regulation. In the case of outsourcing, the financial entity remains fully responsible for fulfilling its incident reporting obligations.

[8] See Article 19(5) of the DORA Regulation. In the case of outsourcing, the financial entity remains fully responsible for fulfilling its incident reporting obligations.

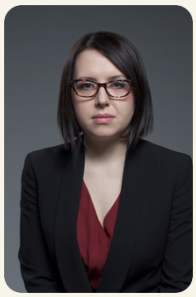
[9] See Article 19(5) of the DORA Regulation. In the case of outsourcing, the financial entity remains fully responsible for fulfilling its incident reporting obligations.

Legance is available to provide any clarifications

For further information:

Gian Paolo Tagariello
SENIOR PARTNER

+39 02.89.63.071
+39 06.93.18.271
gtagariello@legance.it



Armenia Riviezzo
MANAGING ASSOCIATE

+39 06.93.18.271
ariviezzo@legance.it

Luca Benadin
ASSOCIATE

+39 02.89.63.071
lbenadin@legance.it

Contacts

Milano
Via Broletto, 20
20121
T +39 02 89 63 071

Roma
Via di San Nicola da Tolentino, 67
00187
T +39 06 93 18 271

Londra
Aldermary House,
10 – 15 Queen Street
EC4N 1TX
T +44 (0)20 70742211

info@legance.it | www.legance.it

The firm

Legance is an independent Italian law firm with expert, active and result-oriented lawyers, with a strong team spirit that has permitted a flexible and incisive organisational model that, through departments active in all practice areas of business law, offers the right balance between the specialist and the lawyer as a global consultant. Legance comprises more than 400 lawyers, working in its Milan, Rome and London offices, and has a diverse and extensive practice covering the following areas: Administrative; Banking & Finance; Compliance; Corporate Finance; Data Law; Debt Capital Markets; Dispute Resolution; Employment and Industrial Relations; Energy & Infrastructure; Environmental; Equity Capital Markets; ESG and Impact; EU, Antitrust and Regulation; Financial Intermediaries Regulations; Food; Insurance; Intellectual Property; Investment Funds; Life Sciences & Healthcare; Non Performing Loans; Real Estate; Restructuring and Insolvency; Shipping, Aviation and Transportation; Tax; Telecommunications, Media and Technology; White Collar Crimes. For more information, please visit our website: www.legance.com.

Disclaimer