Legance

Newsletter

MARZO 2025

Novità in materia di segnalazioni dei gravi incidenti informatici e delle minacce informatiche nel settore assicurativo

○ Assicurazioni

Lo scorso 14 febbraio, IVASS ha pubblicato la Lettera al Mercato (la "**Lettera**") recante disposizioni operative ai sensi del Regolamento UE 2022/2054 (c.d. DORA – *Digital Operational Resilience Act*) in materia di segnalazione dei gravi incidenti informatici e delle minacce informatiche.

Destinatari della Lettera sono tanto gli intermediari assicurativi[1] quanto le imprese di assicurazione e riassicurazione con sede legale in Italia[2].

Come noto, il Regolamento DORA, in vigore dal 17 gennaio 2025, rappresenta un pilastro fondamentale per garantire la resilienza operativa digitale nel settore finanziario europeo, ovvero la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa per garantire la sicurezza dei sistemi informatici di rete utilizzati dall'entità finanziaria[3], tra cui le imprese di assicurazione. In tal senso, il Regolamento DORA mira a uniformare e rafforzare la gestione dei rischi informatici e tecnologici nel settore finanziario con un focus particolare sulla prevenzione e sul recupero in caso di incidenti informatici.

Nel contesto del suddetto quadro normativo e in virtù degli obblighi già applicabili dal gennaio scorso, la Lettera richiama la normativa rilevante fornendo così agli operatori uno strumento utile per adempiere correttamente alla segnalazione dei gravi incidenti informatici posto che lo stesso Regolamento DORA (cfr. art. 19) richiede alle entità finanziarie di segnalare alle autorità competenti gli incidenti gravi connessi alle TIC (le Tecnologie dell'Informazione e della Comunicazione) e notificare, su base volontaria, le minacce informatiche significative.

Nello specifico, la Lettera richiama i gravi incidenti informatici oggetto di segnalazione così come definiti dal Regolamento Delegato UE 2024/1772 (cfr. art. 8).

La Lettera mira inoltre a precisare le tempistiche che le entità finanziarie devono rispettare in caso di grave incidente informatico posto che i termini per la segnalazione degli incidenti devono seguire un approccio coerente per tutti i tipi di entità finanziaria. In particolare, le fasi della reportistica sono così suddivise:

- una notifica iniziale, al più tardi entro 24 ore dall'identificazione dell'incidente;

un report intermedio, entro 72 ore dalla notifica iniziale con possibilità di trasmettere successivi aggiornamenti;

- un report finale, entro un mese dall'invio dell'ultimo aggiornamento del report intermedio.

Resta inteso che il contenuto delle suddette notifiche varia a seconda della fase dell'incidente. Ebbene, secondo il Regolamento Delegato UE 2025/301 la notifica iniziale dovrebbe essere limitata alle sole informazioni significative. Dopo la notifica iniziale, le autorità dovrebbero ricevere informazioni più dettagliate sull'incidente connesso alla TIC tramite il report intermedio e tutte le informazioni pertinenti attraverso il report finale al fine di consentire alle autorità competenti di esaminare ulteriormente l'incidente[4].

Da ultimo, la Lettera richiama l'attenzione sulla segnalazione, su base volontaria, delle minacce informatiche ritenute rilevanti per il sistema finanziario[5], gli utenti dei servizi o i clienti. Va precisato che le minacce informatiche significative vanno notificate solamente su base volontaria pertanto il contenuto di tali notifiche non può costituire un onere per le entità finanziarie che dovranno sicuramente cooperare con le autorità competenti ma con una frequenza più limitata rispetto alle informazioni richieste per gli incidenti gravi.

L'introduzione di obblighi di segnalazione degli incidenti informatici e procedure per la notifica volontaria delle minacce informatiche significative richiede ai destinatari della Lettera un'adeguata preparazione organizzativa.

Viene altresì richiesta una collaborazione proattiva che sia in grado di garantire un coordinamento efficace nella gestione delle crisi digitali con l'IVASS[6], fermo restando che ai sensi del Regolamento DORA le entità finanziarie possono esternalizzare gli obblighi di segnalazione a un fornitore terzo di servizi[7].

L'attenzione delle autorità competenti è alta e considerato che non vi è stato un periodo di transizione, le autorità di vigilanza sottolineano l'importanza che le entità finanziarie adottino un approccio solido e strutturato al fine di adempiere ai propri obblighi in modo tempestivo. In tal senso, le entità finanziarie sono tenute a identificare e ad affrontare tempestivamente le carenze interne e gli obblighi previsti dal Regolamento DORA anche alla luce delle disposizioni del D. lgs. 23/2025[8] aventi ad oggetto l'adeguamento della normativa nazionale al suddetto Regolamento comunitario. Tra le varie novità, si rammentano infatti le modifiche al Codice delle Assicurazioni Private nella parte relativa alle sanzioni che risultano applicabili in caso di inosservanza di specifiche disposizione del Regolamento DORA, tra cui la mancata segnalazione dei gravi incidenti informatici[9].

[1] In tal senso, si segnala che sono soggetti alla disciplina dora gli intermediari di assicurazione, di riassicurazione e assicurativi a titolo accessorio che hanno un numero di dipendenti superiore a 250 e un fatturato annuo superiore a 50 milioni di euro o un bilancio annuo superiore a 43 milioni di euro.
[2] Tra i destinatari della lettera vi sono anche le sedi secondarie delle imprese di assicurazione con sede legale in uno stato terzo rispetto allo s.e.e..
[3] Cfr. Art. 2 del regolamento dora. Tra le entità finanziarie vi rientrano, *inter alia*, gli enti creditizi, gli istituti di pagamento, le imprese di assicurazione e riassicurazione, gli intermediari assicurativi, gli intermediari riassicurativi e gli intermediari assicurativi a titolo accessorio.
[4] I *template* per ottemperare all'obbligo di segnalare i gravi incidenti e le segnalazioni di minacce informatiche rilevanti sono allegati alla lettera. Le segnalazioni dovranno essere trasmesse all'ivass via pec ai seguenti indirizzi: vigilanza.prudenziale@pec.ivass.it dalle imprese di assicurazione; e vigilanzacondottamercato@pec.ivass.it dagli intermediari di assicurazione, di riassicurazione e assicurativi a titolo accessorio.
[5] L'art. 18 del regolamento dora precisa che le entità finanziarie classificano le minacce informatiche come significative in base alla criticità dei servizi a rischio, comprese le operazioni dell'entità finanziaria, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l'estensione geografica delle aree a rischio.
[6] Ai sensi del d. Lgs. 23/2025, ivass è l'autorità competente a ricevere le segnalazioni dei gravi incidenti informatici e le notifiche volontarie relative alle minacce informatiche significative.
[7] Cfr. Art. 19, par. 5, del regolamento dora. In caso di esternalizzazione l'entità finanziaria rimane pienamente responsabile di espletare gli obblighi di segnalazione degli incidenti.
[8] Il d. Lgs. 23/2025 è stato pubblicato in gazzetta ufficiale l'11 marzo 2025.

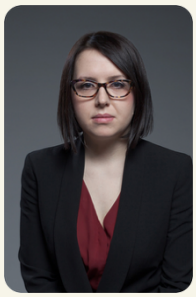
[9] Gli articoli 310, 311-sexies e 324 del codice delle assicurazioni private, così come modificati dal d. Lgs. 23/2025, relativi alle sanzioni, risultano in vigore dal 12 marzo 2025.

Legance è a disposizione per qualsiasi informazione

Per ulteriori informazioni

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

Contatti

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

Lo Studio

Legance è uno studio legale italiano con un team di professionisti esperti, dinamici e orientati al risultato, il cui affiatamento ha reso possibile un modello organizzativo flessibile ed incisivo che, attraverso dipartimenti attivi in tutti i settori della consulenza legale d'affari, esprime il giusto equilibrio tra specialista e avvocato come consulente globale. Legance conta oltre 400 avvocati, nelle sedi di Milano, Roma e Londra. Le aree di competenza sono: Alimentare; Ambientale; Amministrativo; Assicurazioni; Banking; Compliance; Contenzioso, Arbitrati e ADR; Corporate M&A; Data Law; Debt Capital Markets; Energy & Infrastructure; Equity Capital Markets; ESG e Impact; Fashion & Luxury; Financial Intermediaries Regulations; Finanza Strutturata; Fondi di Investimento; Lavoro e Relazioni Industriali; Life Sciences & Healthcare; Navigazione e Trasporti; Penale d'Impresa; Proprietà Intellettuale; Real Estate; Ristrutturazione del Debito e Crisi d'Impresa; Sport; Telecomunicazioni, Media e Tecnologia; Tributario; UE, Antitrust e Regolamentazione. Per maggiori informazioni, potete visitare il nostro sito web: www.legance.it.

Disclaimer