IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

SERVIZIO VIGILANZA PRUDENZIALE
SERVIZIO VIGILANZA CONDOTTA DI MERCATO
SERVIZIO NORMATIVA E POLITICHE DI VIGILANZA

Rifer. a nota n. *del*

Classificazione III 1 3

All.ti n . 2

Alle Imprese di assicurazione e riassicurazione con sede legale in Italia
LORO SEDI
ITALIA

Alle Rappresentanze Generali per l'Italia delle imprese di assicurazione con sede legale in uno Stato terzo rispetto allo S.E.E.
LORO SEDI
ITALIA

Agli intermediari di assicurazione, di riassicurazione e assicurativi a titolo accessorio rilevanti ai fini della normativa DORA (*)

Oggetto Segnalazioni dei gravi incidenti informatici e delle minacce informatiche ai sensi del Regolamento UE 2022/2054 (DORA).

Il Regolamento UE 2022/2554 (c.d. DORA - *Digital Operational Resilience Act*), applicabile dal 17 gennaio 2025, ha introdotto disposizioni per le imprese assicurative e per gli intermediari di assicurazione, di riassicurazione e assicurativi a titolo accessorio rilevanti, avuto riguardo alle segnalazioni di grave incidente informatico e di minacce informatiche, fattispecie per le quali il Regolamento Delegato UE 2024/1772 e i relativi Atti delegati (RTS e ITS) adottati dalla Commissione Europea (di seguito: “Atti delegati”) forniscono ulteriori specifiche disposizioni.

Con riferimento agli incidenti informatici, il Regolamento Delegato UE 2024/1772 definisce grave un incidente che abbia interessato i servizi critici di cui all’art. 6 e che soddisfi una delle seguenti condizioni:

a) i sistemi informatici siano stati oggetto di accessi non autorizzati come descritto all’art. 9, paragrafo 5, lettera b);

b) siano state raggiunte almeno due delle altre soglie di rilevanza definite nell’art. 9 paragrafi da 1 a 6.

* 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.

Gli Atti delegati stabiliscono inoltre le tempistiche delle tre fasi della reportistica all'Autorità competente. In particolare:

1) una notifica iniziale, al più tardi entro 24 ore dall'identificazione dell'incidente;
2) un *report* intermedio, entro 72 ore dalla notifica iniziale, con possibilità di trasmettere successivi aggiornamenti;
3) un *report* finale, entro un mese dall'invio dell'ultimo aggiornamento del *report* intermedio.

Gli Atti delegati indicano anche il contenuto delle notifiche, caratterizzate da un livello di dettaglio crescente.

Infine, il Regolamento DORA (art. 19, comma 2) prevede che le entità finanziarie hanno la possibilità di segnalare all'Autorità competente, su base volontaria, le minacce informatiche ritenute rilevanti per il sistema finanziario, gli utenti dei servizi o i clienti.

Ciò considerato, al fine di consentire alle imprese di assicurazione[1] e agli intermediari soggetti alla normativa DORA di ottemperare all'obbligo di segnalare i gravi incidenti e di trasmettere, eventualmente, le segnalazioni di minacce informatiche rilevanti, si allegano i *template* che dovranno essere compilati secondo le modalità previste dagli Atti delegati.

Le segnalazioni sugli incidenti andranno trasmesse all'IVASS via PEC, nei tempi sopra ricordati, agli 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.

Distinti saluti.

Per delegazione del Direttorio Integrato

Firmato digitalmente da
RICCARDO CESARI

[1] Nelle more dell'adeguamento del Regolamento 38/2018 alle nuove disposizioni DORA, le segnalazioni di un grave incidente informatico secondo le modalità indicate nella presente lettera non dovranno essere trasmesse anche ai fini del rispetto degli obblighi segnaletici/informativi previsti dall'articolo 16 del Reg. 38/2018 in materia di Sistemi informatici e *cyber security*.