Pill: Regolamento DORA - pubblicazioni Banca d'Italia

- **"*Comunicazione al mercato in materia di sicurezza ICT*", pubblicata in data 23 dicembre 2024;**
- **"*Istruzioni operative per la trasmissione dei gravi incidenti ICT e delle minacce informatiche significative attraverso la piattaforma INFOSTAT*", pubblicate in data 27 dicembre 2024.**

Premessa

Come noto, il 17 gennaio 2025 entrerà in vigore il Regolamento sulla resilienza operativa digitale del settore finanziario ("**Regolamento DORA**"). Questo regolamento mira a rafforzare la gestione dei rischi ICT nel settore finanziario a livello europeo.

Banca d'Italia, in linea con la Vigilanza unica europea, sta lavorando per garantire la sicurezza ICT attraverso iniziative di supervisione. Le analisi recenti hanno mostrato un aumento degli incidenti operativi e cibernetici, con particolare attenzione agli accessi non autorizzati che compromettono la riservatezza dei dati.

Comunicazione al mercato in materia di sicurezza ICT

Facendo quindi seguito ai risultati delle recenti analisi in tema di sicurezza ICT, Banca d'Italia ("**Autorità**"), in data 23 dicembre 2024, ha pubblicato una **Comunicazione** per richiamare l'attenzione dei soggetti a cui si applica il Regolamento DORA al rispetto degli obblighi conseguenti all'entrata in vigore della normativa.

Banca d'Italia intende monitorare e supportare gli intermediari finanziari nell'implementazione delle norme DORA attraverso iniziative di supervisione che riguardano sia i singoli operatori finanziari sia il sistema nel suo complesso.

L'Autorità richiede agli intermediari di eBettuare un'autovalutazione del proprio sistema di gestione dei rischi ICT e di trasmettere i risultati di tale autovalutazione **entro il 30 aprile 2025**.

Inoltre, Banca d'Italia si riserva di emanare una specifica comunicazione al mercato sull'attuazione nazionale del Regolamento DORA, richiamando l'attenzione degli intermediari sulle evidenze emerse dalle analisi di supervisione.

Ciò premesso, più nello specifico, l'Autorità ha richiesto di **valutare**, su base consolidata per i gruppi e individuale per i soggetti non appartenenti a gruppi, **il proprio posizionamento rispetto ai requisiti normativi introdotti**, con particolare riferimento a:

(i) strategie di gestione del rischio ICT di terze parti, rinnovo dei contratti di fornitura e trasmissione all'Autorità del Registro delle Informazioni;
(ii) adattamento di presidi e politiche interne;
(iii) attività e programmi di test di resilienza digitale.

L'Autorità ha, inoltre, richiesto di effettuare un'**autovalutazione del proprio sistema di gestione dei rischi ICT**, al fine di assicurare che le politiche, le procedure, i protocolli e gli strumenti in materia ICT siano adeguati a:

- prevenire, ovvero rilevare tempestivamente, violazioni alla riservatezza dei dati e/o dei servizi forniti;
- ridurre il rischio derivante dai cambiamenti ICT, attraverso una valutazione del proprio quadro *ICT change management*.

Tale autovalutazione, come accennato, una volta approvata dall'organo di amministrazione con il coinvolgimento delle funzioni di controllo di secondo e terzo livello, deve essere trasmessa all'Autorità entro il 30 aprile 2025.

Per visionare la Comunicazione di Banca d'Italia del 23 dicembre 2024, cliccare qui.

***

Istruzioni operative per la trasmissione dei gravi incidenti ICT e delle minacce informatiche significative attraverso la piattaforma INFOSTAT

In data 27 dicembre 2024, Banca d'Italia ha pubblicato le istruzioni operative attraverso cui gli intermediari potranno segnalare, tramite la piattaforma INFOSTAT, i **gravi incidenti ICT**, nonché, su base volontaria, le **minacce informatiche significative** ("**Istruzioni operative**").

Inoltre, l'Autorità ha messo a disposizione dei destinatari (e quindi degli intermediari dalla medesima direttamente vigilati che rientrano nell'ambito di applicazione soggettivo del Regolamento DORA) i modelli attraverso cui sarà possibile effettuare le segnalazioni.

In particolare:

- per la segnalazione dei gravi incidenti ICT, dovrà essere utilizzato il modello di segnalazione denominato "DORA_modello_segnalazione_incidenti.xslx";
- per la segnalazione volontaria delle minacce informatiche significative, dovrà essere utilizzato il modello di segnalazione denominato "DORA_modello_segnalazione_minacce_informatiche.xslx".

Il documento fornisce informazioni specifiche in merito alle modalità standardizzate di compilazione dei moduli.

Per consultare le Istruzioni operative per la compilazione e trasmissione dei gravi incidenti ICT e delle minacce informatiche significative del 27 dicembre 2024, cliccare qui.