PAVESIO E ASSOCIATI
WITH NEGRI-CLEMENTI

CLIENT ALERT
Dicembre 2023

Regolamento DORA: il 2024 anno di implementazione per banche, assicurazioni, finanziarie e fornitori ICT

Nel più ampio contesto delle direttive NIS del 2016 e NIS 2 del 2023, **il 17 gennaio 2023 è entrato in vigore del Regolamento EU 2022/2554 c.d. DORA (Digital Operational Resilience Act)** che rappresenta una svolta nel settore finanziario con l'obiettivo di rafforzare ed armonizzare a livello europeo i principali requisiti di cybersecurity per le società finanziarie come banche, compagnie di assicurazione, società di servizi di criptovalute, istituzioni finanziarie ed i loro fornitori.

Recentemente, inoltre, le Autorità di vigilanza europee (EBA, EIOPA ed ESMA, insieme le ESAs) **hanno avviato una consultazione pubblica su un primo gruppo di standard tecnici** (RTS e ITS) di attuazione del Regolamento che coprono aree chiave come la gestione del rischio ICT, la gestione e la segnalazione degli incidenti legati all'ICT, i test di resilienza operativa digitale e la gestione del rischio ICT derivanti da terzi. La DORA ha incaricato le ESAs di sviluppare congiuntamente 13 standard tecnici.

Il Regolamento DORA fa parte di una più ampia strategia digital europea che mira a garantire che le imprese del settore siano in grado di affrontare gli attacchi informatici e le complessità operative attraverso l'implementazione di misure di governance, cybersecurity e gestione del rischio ICT, nonché segnalazione degli incidenti e condivisione delle criticità che garantiscano una stabilità del sistema e di cui anche l'EU Artificial Intelligence Act rappresenta un ulteriore tassello in evoluzione.

Di seguito un'analisi delle previsioni più rilevanti del regolamento DORA.

1. Obbiettivi, contenuti ed ambito di applicazione

Perché un regolamento specifico?

L'utilizzo di tecnologie dell'informazione e comunicazione (ICT) ha rivoluzionato il settore finanziario e acquisito un ruolo critico, anche a seguito di una crescente complessità dell'operatività e dell'utilizzo sempre più intenso di fornitori specializzati esterni al perimetro regolamentare. In questo contesto, il pericolo di conseguenze sistemiche e le lacune del quadro normativo hanno portato al concepimento del Regolamento DORA, che si prefigge di regolare in maniera uniforme la "resilienza operativa" nel settore finanziario in Europa. L'obiettivo è, quindi, di imporre l'adozione di requisiti di sicurezza e governance standardizzati, necessari a garantire che le entità finanziarie che operano in Europa siano poste nelle condizioni di prevenire, resistere e reagire alle minacce informatiche di cui potrebbero essere bersaglio, in questo modo estendendo anche il perimetro regolamentare a tutti i soggetti coinvolti e creando un coordinamento su quest'area tra tutte le Authorities regolamentari.

A chi si applica?

Il Regolamento DORA si applica (art. 2) a tutti gli operatori tradizionali del settore finanziario, quali banche, finanziarie, imprese di investimento ed assicurazioni, ma anche ai nuovi attori del mercato quali fornitori di servizi per le cripto-attività e di crowfunding, nonchè ai fornitori di servizi ICT.

Quando sarà operativo?

Gli operatori interessati hanno 24 mesi dalla data di entrata in vigore del Regolamento per attuare tutti gli adempimenti necessari per conformarsi alla normativa.

2. I pilastri del Regolamento DORA

Il Regolamento DORA può essere sintetizzato nei seguenti pilastri principali:

A) Governance ed organizzazione (art. 5)

Le entità finanziarie dovranno dotarsi di una governance dedicata interna e di un quadro di controllo tali da garantire una gestione efficace e prudente di tutti i rischi ICT, al fine di raggiungere un elevato livello di resilienza operativa digitale. L'organo di gestione dell'ente finanziario è il principale responsabile della gestione complessiva dei rischi ICT.

B) Gestione dei rischi informatici – Risk management (artt. 6-16)

Le entità finanziarie dovranno disporre di un quadro di gestione del rischio solido, completo e ben documentato come parte del loro sistema complessivo di gestione del rischio. Tra le altre cose, gli operatori dovranno avere cura di:

- utilizzare strumenti e sistemi di ICT resilienti, tali da ridurre al minimo l'impatto dei relativi rischi
- identificare prontamente tutte le fonti di rischio ed implementare meccanismi in grado di rilevare attività anomale
- adottare procedure interne e misure di protezione e prevenzione

C) Gestione, classificazione e segnalazione degli incidenti informatici (artt. 17-23)

In materia di gestione degli incidenti legati ai servizi ICT, le entità finanziare dovranno:

- prevedere ed implementare politiche di continuità operativa, nonchè sistemi e piani di ripristino in caso di disastro;
- dotarsi di capacità e personale idonei a rilevare vulnerabilità, minacce, incidenti e attacchi informatici e valutare le possibili conseguenze sulla loro resilienza operativa digitale;
- prevedere piani di comunicazione nei confronti dei vari stakeholder.

Per quanto concerne, inoltre, la segnalazione degli incidenti connessi, le entità finanziarie dovranno stabilire e attuare un processo di gestione per monitorare e registrare gli incidenti connessi alle ICT, per classificarli e determinarne l'impatto e segnalarli, tramite una relazione, alle autorità competenti se ritenuti gravi.

D) Test di resilienza digitale (artt. 24-27)

Il Regolamento DORA introduce un programma di test di resilienza operativa digitale come vero e proprio sistema che comprende una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare. In particolare, al fine di valutare la preparazione alla gestione degli incidenti, di identificare punti deboli, carenze

e lacune della resilienza operativa digitale e di attuare tempestivamente misure correttive, le entità finanziare saranno obbligate a svolgere periodicamente test adeguati. Pertanto, in questo contesto anche i fornitori di servizi terzi dovranno dimostrare di avere le caratteristiche minime per permettere all'entità finanziaria di rispettare il Regolamento DORA ed i requisiti richiesti per lo svolgimento dei test.

E) Gestione dei fornitori di servizi ICT: principi fondamentali, contrattualistica, controlli e quadro di sorveglianza (artt. 28-44)

Al fine di mitigare i rischi derivanti dalla dipendenza delle entità finanziarie da fornitori terzi di servizi, è previsto il conferimento alle autorità di vigilanza finanziaria di specifici poteri di sorveglianza. Pertanto, oltre a prevedere un quadro di sorveglianza a livello europeo per i fornitori terzi di servizi ICT critici, saranno armonizzati gli aspetti contrattuali chiave (stipula, esecuzione, fase post-contrattuale) per garantire che le società finanziarie monitorino i rischi ICT di terzi, inclusa la catena dei sub-fornitori. Inoltre, al fine di garantire l'adeguato monitoraggio dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario, per ciascun fornitore terzo di servizi ICT critico sarà definita una autorità di sorveglianza "capofila".

Vi sono, da ultimo, gli **articoli dal 45 al 64** che regolano i rapporti tra le autorità, i meccanismi di condivisione delle informazioni tra le stesse, l'apparato sanzionatorio e le disposizioni finali.

3. Principali conseguenze per gli operatori e prossimi passi

Da prassi consolidata in numerose altre normative, il Regolamento DORA rimanda ai fini dell'applicazione al **principio di proporzionalità** (art. 4) e, quindi, rimette al singolo soggetto l'onere di valutare e dimostrare il corretto livello dei requisiti che devono essere implementati.

Come prepararsi al Regolamento DORA?

Da questa analisi generale, si evince chiaramente la complessità della governance di tali tematiche che devono essere affrontate in maniera integrata lavorando sulle leve di organizzazione, ruoli e responsabilità, processi, strumenti e contrattualistica. In particolare, sono richieste competenze progettuali, informatiche, legali e di governance.

Sarà quindi fondamentale per tutte le entità finanziarie adottare un approccio proattivo e consapevole, attraverso lo svolgimento di attività preparatorie che consentano di determinare l'effettivo impatto di DORA sulla propria organizzazione e di non trovarsi quindi impreparate al momento della sua applicazione. Tra queste, in particolare, sarà opportuno per gli operatori:

1. **gap analysis della governance e del risk management framework**: aggiornare la struttura di governance interna e le misure di gestione dei rischi ed incidenti ICT già adottate, per verificare la consapevolezza aziendale rispetto al nuovo impianto normativo e valutare se le risorse, le strategie ed i piani di risposta e di ripristino in essere rispondano adeguatamente ai requisiti normativi, allocando in modo integrato compiti e responsabilità;

2. **revisione dei meccanismi di incident reporting**: valutare le capacità e la reattività dell'azienda in ambito di reportistica, e di conseguenza adeguare le esistenti procedure di segnalazione degli incidenti, al fine di garantire un allineamento con i nuovi requisiti normativi;

3. **valutazione dei fornitori critici di servizi ICT, definizione di un processo di selezione, monitoraggio e potenziale exit strategy - rinegoziazione dei contratti ed individuazione clausole critiche**: mappare i contratti con i fornitori terzi di ICT, valutandone la criticità rispetto all'operatività del business, revisionando e documentando le loro vulnerabilità

per permettere la pianificazione di adeguate strategia di contenimento del rischio e rinegoziando gli obblighi delle parti per renderli conformi a quanto previsto dal regolamento.

A loro volta, **anche i fornitori di servizi ICT dovranno valutare la propria appartenenza alla categoria dei fornitori definiti "critici" e, soprattutto in caso positivo, analizzare le azioni da intraprendere** per adeguarsi al nuovo quadro normativo, soddisfare le nuove esigenze di supervisione da parte delle Autorità europee di Vigilanza, nonché interagire in modo proattivo con le entità finanziarie partner.

Le tempistiche del Regolamento DORA

Il regolamento DORA è entrato in vigore il 17 gennaio 2023, ma **diventerà vincolante a decorrere dal 17 gennaio 2025**. Nel mentre il quadro giuridico sarà progressivamente completato da standard tecnici regolatori che saranno sviluppati da ESMA e saranno finalizzati nel corso del 2024.

Contatti

Torino Corso Vittorio Emanuele II, 68 10121 | T. +39 011 51121
Milano Via Bigli 2, 20121 | T. +39 02 303049
Roma Via Ludovisi, 35 00187 | T. +39 011 51121

info@pavesioassociati.it – www.pavesioassociati.it

Per maggiori informazioni:
AreaCompliance@pavesioassociati.it
AreaFinance@pavesioassociati.it

Disclaimer

Il presente documento è redatto in termini generali, unicamente a fini divulgativi e di aggiornamento normativo.