DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Regolamento DORA: analisi dei principali adempimenti

23 Gennaio 2023

Stefano Mele, Partner, Gianni & Origoni
Flavia Bavetta, Associate, Gianni & Origoni

Stefano Mele, Partner, Gianni & Origoni

Flavia Bavetta, Associate, Gianni & Origoni

Stefano Mele

Stefano Mele è Partner dello studio Gianni & Origoni. Responsabile del Dipartimento di Cybersecurity e co-Responsabile del Dipartimento Privacy dello studio Gianni & Origoni. Esperto in materia di ICT, Privacy & Cybersecurity Law. Ha maturato venti anni di esperienza su questioni relative al proprio ambito di operatività e ha prestato la propria assistenza per importanti operazioni riguardanti questioni legali complesse e su più giurisdizioni in materia di nuove tecnologie e privacy, nonché su sicurezza cibernetica e crisis management a seguito di attacchi cyber. È membro del Consiglio Direttivo e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano, oltre che Presidente del "Gruppo di lavoro sulla Cybersecurity" della Camera di Commercio americana in Italia (AmCham).

Il 27 dicembre 2022 è stato pubblicato in Gazzetta Ufficiale il Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (di seguito "**DORA**" o "**Regolamento**").

Il Regolamento è entrato in vigore su tutto il territorio dell'Unione Europea il 17 gennaio 2023. Il legislatore, tuttavia, concede ai soggetti destinatari della norma di adempiere ai numerosi obblighi – di seguito meglio dettagliati – entro il 17 gennaio 2025.

A chi si rivolge la normativa

Il Regolamento si rivolge a un ampio novero di operatori finanziari, quali enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, repertori di dati sulle negoziazioni, gestori di fondi di investimento alternativi, società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di *rating* del credito, amministratori di indici di riferimento critici, fornitori di servizi di *crowdfunding*, repertori di dati sulle cartolarizzazioni.

Inoltre, il DORA si applica ai fornitori di servizi di tecnologie dell'informazione e della comunicazione (ICT).

I principali adempimenti

Dall'analisi complessiva del dettato normativo emergono numerosi obblighi a cui gli operatori finanziari devono adempiere, tra cui a titolo esemplificativo e non esaustivo:

1. adottare un quadro di *governance* e organizzazione interna, che garantisca un controllo efficace e prudente di tutti i rischi ICT. A tal fine, è necessario attribuire specifici compiti all'"organo di gestione" dell'ente finanziario, il quale deve essere incaricato dell'approvazione e applicazione di tutte le disposizioni relative al suddetto quadro, essendone, peraltro, pienamente responsabile;

vedi l'articolo online

2. adottare un piano per la gestione dei rischi informatici, che richiede agli operatori finanziari di:

   - stabilire i requisiti volti all'armonizzazione delle regole di gestione dei rischi relativi alle tecnologie ICT in ogni fase del loro ciclo di vita, con una visione *end-to-end* dei processi aziendali;

   - creare un *ICT Risk Management Framework*;

   - definire una strategia di resilienza digitale in materia di *business continuity* e *disaster recovery*;

3. classificare gli incidenti connessi ai fornitori ICT e le minacce informatiche secondo i criteri indicati dal legislatore, al fine di armonizzare le attività di segnalazione degli incidenti ICT. In particolare, secondo quanto indicato nel Regolamento, le entità finanziarie devono classificare le minacce informatiche in base alla criticità dei servizi a rischio, ivi comprese le operazioni dell'ente, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l'estensione geografica delle aree a rischio;

4. creare un sistema di segnalazione degli incidenti informatici, attuando un processo di monitoraggio, registrazione e gestione costante degli incidenti connessi alle tecnologie ICT, al fine di notificarli alle autorità competenti. Nel merito, il DORA richiede agli operatori finanziari di stabilire procedure per identificare, tracciare, registrare, categorizzare e classificare gli incidenti connessi alle tecnologie ICT in base alla loro priorità, gravità e criticità dei servizi colpiti, di assegnare ruoli e responsabilità al personale interno, nonché di elaborare piani per la comunicazione al personale, ai portatori di interessi esterni, ai mezzi di comunicazione e ai clienti. In ultimo, devono essere stabilite procedure di risposta agli incidenti connessi alle tecnologie ICT per attenuarne l'impatto e garantirne tempestivamente l'operatività e la sicurezza dei servizi;

5. svolgere *test* di resilienza operativa digitale, secondo un approccio *risk-based* e proporzionale rispetto alle dimensioni, alla tipologia di attività e al profilo di rischio dell'operatore finanziario;

6. adottare un sistema di gestione dei rischi informatici derivanti da terzi. In particolare, in tale adempimento rientrano l'identificazione, la classificazione e la documentazione di tutti i processi dipendenti da fornitori terzi di servizi legati alle tecnologie ICT. Inoltre, il DORA richiede l'imposizione di diversi obblighi contrattuali, al fine di garantire un adeguato monitoraggio delle attività svolte da parte dei suddetti fornitori sui servizi tecnologici che assolvono una funzione critica per l'attività svolta da parte dell'ente finanziario;

7. prevedere protocolli di *information sharing*, con l'obiettivo di incoraggiare lo scambio di informazioni sulle minacce informatiche tra le entità finanziarie. In particolare, il DORA prevede l'istituzione di un programma su base volontaria che consenta agli attori finanziari di prevedere accordi per la condivisione e lo scambio di informazioni di *cyber threat intelligence*.

Misure sanzionatorie

In relazione al quadro sanzionatorio, si precisa che seppur il Regolamento detti i criteri di calcolo delle sanzioni, la loro specifica identificazione è lasciata alle autorità competenti.

Pertanto, per comprenderne con precisione la portata sarà necessario monitorare le posizioni e le indicazioni che saranno fornite dalle Autorità europee di Vigilanza.

Cosa fare

Anche solo dall'analisi dei principali adempimenti previsti dal nuovo quadro normativo, risulta molto chiara la mole di attività che dovranno essere ottemperate entro il 17 gennaio 2025.

Pertanto, si ritiene necessario procedere quanto prima con la predisposizione di un piano di adeguamento che consenta di determinare l'effettivo impatto del DORA sulla propria organizzazione.

In aggiunta, non possono essere sottovalutate le interconnessioni con le altre discipline in materia di *cybersecurity*. Infatti, l'impianto del Regolamento DORA risulta combinarsi con molte altre normative sia a livello europeo (*i.e.* Direttiva NIS 1, Direttiva NIS 2, TIBER EU Framework, EBA Guidelines, MIFID II, GDPR, Basel Committee's 2021 Principles on Operational Resilience, EIOPA Guidelines), che nazionale (*i.e.* il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), la Circolare 285 di Banca d'Italia, il Regolamento IVASS).

In tal senso, quindi, si ritiene che gli attori del settore finanziario, a titolo esemplificativo e non esaustivo, debbano tenere conto e raccordare le diverse procedure e tempistiche di comunicazione degli incidenti imposte contestualmente dal DORA, dalla Direttiva NIS 1 e dalla (futura) Direttiva NIS2, nonché dal Perimetro di Sicurezza Nazionale Cibernetica. Inoltre, considerato che il DORA richiede l'applicazione di misure di sicurezza potenzialmente non coincidenti rispetto a quelle già implementate da alcuni attori ai sensi della Direttiva NIS 1 e del PSNC, potrebbe essere necessario procedere ad un *assesment* per comprendere l'esatto *scope* applicativo delle tre normative. In aggiunta a quanto sopra, i requisiti di sicurezza imposti dalla Circolare 285 di Banca d'Italia potrebbero non essere più sufficienti a soddisfare le richieste del Regolamento.

Alla luce di ciò, appare evidente come la sfida più complessa per gli operatori del settore sia senz'altro proprio quella di valutare gli adempimenti già svolti ai sensi delle normative precedentemente emanate, al fine di comprendere, in un'ottica di efficienza operativa sul piano tecnico, legale e dei processi interni, i punti di intersezione e raccordo. Soltanto successivamente, quindi, si potrà procedere con le attività richieste dal legislatore europeo attraverso questo importantissimo Regolamento.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it