lawalert

30 gennaio
2 0 23

Regolamento DORA, direttiva NIS2 e direttiva CER
Gli ultimi provvedimenti EU in materia di Cybersecurity

In data 27 dicembre 2022 sono state pubblicate sulla Gazzetta Ufficiale dell'Unione Europea tre nuovi provvedimenti (un Regolamento e due direttive) che contribuiscono a espandere l'attuale quadro normativo europeo in materia di cybersicurezza:

I. il Regolamento (UE) 2022/2554 del 14 dicembre 2022 (Digital Operational Resilience Act o **"DORA"**) in tema di resilienza operativa digitale per il settore finanziario;

II. la direttiva (UE) 2022/2555 (o **"NIS 2"**) che mira a garantire un livello comune elevato di cybersicurezza nell'Unione, e che abroga la precedente direttiva NIS (UE) 2016/1148, e

III. la direttiva (UE) 2022/2557 del 14 dicembre 2022 (Critical Entities Resilience o **"CER"**) relativa alla resilienza cyber dei soggetti considerati critici.

Tali nuove regolamentazioni, seppur con focus e ambiti di applicazione differenti, hanno lo scopo comune di rafforzare e completare il quadro normativo della EU Cybersecurity Strategy presentata in data 16 dicembre 2020 dalla Commissione europea e dall'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, e finalizzata a rafforzare la resilienza alle minacce informatiche e a garantire che i cittadini e le imprese possano beneficiare di tecnologie digitali affidabili.

DORA

Il Regolamento (UE) 2022/2554 del 14 dicembre 2022 (Digital Operational Resilience Act o "DORA") consolida e armonizza i requisiti di cybersicurezza per le entità finanziarie dell'Unione Europea e trova applicazione nei confronti di enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti, provider di moneta elettronica, imprese di investimento ed altri soggetti elencati all'articolo 2 (che indica altresì le entità nei confronti delle quali, invece, il DORA non troverà applicazione o che dovrebbero essere soggette ad adempimenti cyber semplificati).

La prima Direttiva NIS aveva già introdotto un modello di identificazione nazionale degli Operatori di Servizi Essenziali (o "OSE") includendo tra gli altri enti creditizi e operatori finanziari.

La Direttiva NIS2 ha invece stabilito un criterio uniforme basato sulla soglia dimensionale per stabilire quali entità rientrano nel suo ambito di applicazione, mantenendo nel contempo al suo interno anche le attività finanziarie.

Il considerando 16 del DORA stabilisce che lo stesso costituisce una lex specialis rispetto alla direttiva NIS2, poiché in relazione al settore finanziario definisce i requisiti di gestione dei rischi informatici e segnalazione di incidenti connessi alle TIC [1] (ossia ai software o hardware presenti nei sistemi informatici e di rete utilizzati dall'entità finanziaria). Il DORA è finalizzato in particolare a prevenire e attenuare i rischi relativi alla sicurezza informatica.

I soggetti rientranti nell'ambito di applicazione del DORA dovranno predisporre un quadro per la gestione rapida, efficace ed esaustiva dei rischi informatici (anche derivati da terzi), utilizzare ed aggiornare su base regolare i propri sistemi e protocolli informatici, identificare tutte le funzioni commerciali supportate dai propri strumenti informatici, monitorare il funzionamento dei propri strumenti informatici, inserire le clausole indicate dal DORA nei propri contratti con fornitori di servizi informatici e adottare policy dedicate per garantirne la sicurezza e la continuità operativa, meccanismi per individuare eventuali attività anomale e punti di vulnerabilità potenziali, procedure di backup, nonché un programma di test di resilienza operativa digitale.

In aggiunta, è previsto che le entità finanziarie siano altresì tenute a raccogliere informazioni in relazione alle vulnerabilità e alle minacce informatiche ed agli attacchi informatici classificandoli ed analizzando i probabili effetti che questi possono avere sulla propria resilienza operativa digitale ed a determinati obblighi di comunicazione interna ed esterna.

[1] La Direttiva NIS2 distingue servizi, prodotti e processi TIC (nella traduzione italiana della direttiva resta TIC invece che ICT).
- «prodotto TIC»: un elemento o un gruppo di elementi di una rete o di un sistema informativo;
- «servizio TIC»: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;
- «processo TIC»: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC.

Il DORA prevede inoltre che l'Agenzia Europea per la cybersicurezza ("ENISA"), la Banca Centrale Europea e le Autorità Europee di Vigilanza ("AEV"), alle quali il DORA stesso attribuisce compiti di sorveglianza, elaborino norme tecniche di regolamentazioni comuni.

Il considerando 38 del DORA prevede che alle imprese finanziarie di maggiori dimensioni venga imposta l'introduzione di meccanismi di governance più complessi rispetto a quelli previsti per le società considerate microimprese ai sensi del DORA stesso.

Questa previsione nasce dalla considerazione che tali imprese siano dotate di risorse più ampie di cui disporre per sviluppare strutture di governance ed elaborare strategie aziendali dedicate.

È inoltre previsto che i contratti tra le entità finanziarie e i fornitori di servizi TIC debbano garantire la copertura delle principali disposizioni contrattuali previste dal DORA stesso (principalmente all'articolo 30).

Il DORA troverà applicazione a partire dal 17 gennaio 2025.

NIS 2

La direttiva (UE) 2022/2555 (o "NIS 2"), nell'abrogare e sostituire la direttiva (UE) 2016/1148 (o "NIS") amplia il proprio campo di applicazione distinguendo tra "entità essenziali" e "importanti", con differenti regimi di vigilanza, nei settori ad "elevata criticità" elencati nell'allegato I e negli "altri settori critici" elencati all'allegato II, introducendo una regola di dimensionamento come regola generale.

Per quanto riguarda i settori ad elevata criticità, oltre a quelli già ricompresi nell'ambito di applicazione della precedente direttiva NIS - ossia energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, infrastrutture digitali - sono stati infatti inclusi anche i settori delle acque reflue, della gestione dei servizi TIC (business-to-business), della Pubblica amministrazione e dello spazio.

Sono invece considerati "altri settori critici" indicati nell'Allegato II i seguenti settori: servizi postali e di corriere, gestione dei rifiuti, fabbricazione produzione e distribuzione di sostanze chimiche, produzione trasformazione e distribuzione di alimenti, fabbricazione (ad esempio di dispositivi medici, di computer, di apparecchiature elettriche et cetera), fornitori digitali (ossia di mercati online, motori di ricerca online, piattaforme di servizi di social network), e le organizzazioni di ricerca.

I soggetti rientranti nell'ambito di applicazione della Direttiva NIS 2 dovranno presentare determinate informazioni alle autorità competenti in relazione ai loro obblighi di registrazione, e dovranno adottare determinate misure (ad esempio, misure relative alla gestione degli incidenti, alla continuità operativa, alla sicurezza della catena di approvvigionamento, alla sicurezza delle risorse umane, alle politiche di controllo degli accessi e alla gestione degli asset) per gestire i rischi per la sicurezza della rete e dei sistemi informativi.

Gli organi direttivi deli Enti (sia essenziali che importanti) dovranno approvare e supervisionare l'attuazione delle misure di gestione del rischio di cybersecurity. Inoltre, i membri della governance dovranno seguire una formazione specifica e spingere la propria società a offrire regolarmente una formazione simile ai propri dipendenti. Viene anche introdotta la responsabilità dei vertici aziendali per il mancato rispetto degli obblighi di sicurezza informatica.

L'articolo 3 della NIS 2 prevede che gli Stati membri dell'Unione Europea definiscano entro il 17 aprile 2025 un elenco dei soggetti definiti essenziali ed importanti ai sensi della NIS stessa, nonché dei soggetti che forniscono servizi di registrazione dei nomi a dominio e che tale elenco sia successivamente riesaminato e, se opportuno, integrato almeno ogni due anni.

Gli Stati Membri sono tenuti a recepire le disposizioni della NIS 2 nei rispettivi diritti nazionali entro il 17 ottobre 2024.

CER

La direttiva (UE) 2022/2557 del 14 dicembre 2022 (Critical Entities Resilience o "CER") relativa alla resilienza dei soggetti critici, sostituirà la direttiva 2008/114/CE, che era limitata ai settori dell'energia e dei trasporti, e coprirà undici nuovi settori (energia, trasporti, banche, infrastrutture dei mercati finanziari [2], salute, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio e produzione, trasformazione e distribuzione di alimenti).

Entro il 17 luglio 2026, ogni Stato membro dovrà individuare gli enti critici per i settori e i sottosettori indicati dalla direttiva.

Entro nove mesi dalla loro identificazione, i soggetti identificati dovranno effettuare una valutazione del proprio livello di rischio, che dovrà essere rinnovata successivamente ogni quattro anni, per valutare eventuali rischi che potrebbero interrompere la fornitura dei propri servizi essenziali.

I soggetti individuati dovranno adottare misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la loro resilienza, sulla base delle informazioni pertinenti fornite dagli Stati membri nella loro valutazione generale del rischio e dei risultati della valutazione del rischio del singolo soggetto critico.

I soggetti individuati che rientrano nell'ambito di applicazione delle nuove norme dovranno inoltre notificare all'autorità competente, senza indebito ritardo, gli incidenti che interrompono in modo significativo o che potrebbero interrompere in modo significativo la fornitura di servizi essenziali.

Le autorità competenti, a seguito delle azioni di vigilanza (ispezioni in loco, audit) o della valutazione delle informazioni richieste, possono ordinare ai soggetti critici interessati di adottare le misure necessarie e proporzionate per porre rimedio a qualsiasi violazione individuata e di fornire alle autorità informazioni sulle misure adottate.

[2] Alcune disposizioni della Direttiva CER non si applicheranno ai soggetti appartenenti a questi settori, poiché coperti dalla DORA per le infrastrutture bancarie e dei mercati finanziari e dalla Direttiva NIS 2 per le infrastrutture digitali.

RIASSUMENDO

Soggetti coinvolti

Entità finanziarie (elencate all'art. 2 del DORA).

Tra cui 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 autorizzati ed emittenti di token collegati ad attività; depositari centrali di titoli; gestori di fondi di investimento alternativi, società di gestione; fornitori di servizi di comunicazione dati; imprese di assicurazione e di riassicurazione; intermediari assicurativi; 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; fornitori terzi di servizi TIC.

Soggetti appartenenti ai settori ad alta criticità e agli altri settori come definiti agli allegati I e II della NIS 2.

Settori ad alta criticità: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC (business-to-business), Pubblica amministrazione e spazio.

Altri settori critici: servizi postali e di corriere, gestione rifiuti, fabbricazione, produzione e distribuzione di sostanze chimiche, produzione trasformazione e distribuzione di alimenti, fabbricazione (ad esempio di dispositivi medici, di computer, di apparecchiature elettriche et cetera), fornitori digitali (ossia di mercati online, motori di ricerca online, piattaforme di servizi di social network), e organizzazioni di ricerca.

La CER si applica ai soggetti critici che saranno individuati dai singoli Stati Membri entro il 17 luglio 2026.

Tali soggetti operano nei seguenti settori: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, enti della Pubblica Amministrazione, spazio, produzione, trasformazione e distribuzione di alimenti.

Attività che tali soggetti dovranno porre in essere

- Gestire i rischi delle tecnologie dell'informazione e della comunicazione;
- Segnalare alle autorità competenti gli incidenti gravi connessi alle TIC e inviare notifiche su base volontaria in relazione alle minacce informatiche significative;
- Segnalare alle autorità competenti gravi incidenti operativi o relativi alla sicurezza dei pagamenti;
- Effettuare test di resilienza operativa digitale;
- Condividere dati e informazioni in relazione alle vulnerabilità e alle minacce informatiche;
- Adottare misure relative alla solida gestione dei rischi informatici derivanti da terzi;
- Rispettare gli obblighi relativi agli accordi contrattuali stipulati con i fornitori terzi di servizi informatici.

- Adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi,
- Rispettare gli obblighi di segnalazione degli incidenti informatici,
- Utilizzare, ove previsto, solo fornitori di prodotti, processi e servizi TIC certificati,
- Rispettare, ove previsto, gli obblighi informativi importi a determinati soggetti (come registri di nomi a dominio, soggetti che forniscono servizi di registrazione dei nomi a dominio, fornitori di servizi di Cloud computing *et cetera*).

- Effettuare, entro nove mesi dalla loro identificazione, una valutazione del proprio livello di rischio, che dovrà essere rinnovata successivamente ogni quattro anni, per valutare eventuali rischi che potrebbero interrompere la fornitura dei propri servizi essenziali,
- Adottare misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la loro resilienza, sulla base delle informazioni pertinenti fornite dagli Stati membri nella loro valutazione generale del rischio e dei risultati della valutazione del rischio del singolo soggetto critico,
- Notificare all'autorità competente, senza indebito ritardo, gli incidenti che interrompono in modo significativo o che potrebbero interrompere in modo significativo la fornitura di servizi essenziali.

SANZIONI

Per quanto riguarda il DORA, Gli stati membri avranno facoltà di identificare le sanzioni penali, amministrative e misure di riparazione applicabili. Le autorità competenti avranno tutte poteri di supervisione, indagine e sanzione necessari per adempiere ai propri doveri.

Con riguardo alla NIS 2, rimane in vigore un sistema sanzionatorio simile a quello della precedente NIS. in caso di violazione di determinati obblighi, le imprese che rientrano nel campo di applicazione della NIS 2 possono essere soggette all'applicazione di sanzioni fino a Euro 10 milioni o al 2% del fatturato globale dell'anno precedente in caso di società essenziali, mentre sanzioni fino a Euro 7 milioni o al 1,4% del fatturato globale in caso di società importanti.

La CER prevede che gli Stati membri stabiliscano sanzioni effettive, proporzionate e dissuasive applicabili in caso di violazione delle misure nazionali adottate, prendendo tutte le misure necessarie per assicurarne l'attuazione.

COSA FARE

Visti i nuovi testi normativi, e anche alla luce di una normativa nazionale specifica, il nostro consiglio è di agire subito e di valutare in particolare quanto segue:

- valutare se l'impresa rientra o potrebbe rientrare nel campo di applicazione della nuova normativa;
- Quali nuovi requisiti dovranno essere implementati nel caso in cui si rientri direttamente nel campo di applicazione della nuova legislazione;
- Se l'impresa non rientra direttamente nell'ambito di applicazione della nuova normativa, valutare se eventuali fornitori o clienti sono soggetti alle nuove norme;
- Quali obblighi le imprese devono inserire contrattualmente a carico dei propri fornitori per facilitare una supply chain senza soluzione di continuità e conforme alla cybersecurity alla normativa applicabile;
- Preparare/aggiornare le policy interne per la segnalazione di incidenti e minacce;
- Sarà importante verificare se gli Stati membri in cui si opera non impongano l'uso di prodotti, servizi o processi certificati. Pertanto, la conoscenza degli obblighi normativi sarà rilevante anche per le imprese non direttamente coperte dal nuovo atto legislativo;
- Valutare se ci sono requisiti di sicurezza informatica locali correlati o aggiuntivi, che devono ancora o potenzialmente essere implementati a causa di una legislazione nazionale, al fine di orientare un approccio coordinato in termini di implementazione.

***

Questo articolo è redatto a scopo informativo. Non si tratta di un parere legale esaustivo in materia di Cybersicurezza. Per eventuali ulteriori informazioni e approfondimenti specifici vi invitiamo a contattare Roberto.Camilli@bdo.it, Gabriele.Ferrante@bdo.it, Sofia Ferri Sofia.Ferri@bdo.it e Giulia Nobile Giulia.Nobile@bdo.it.

Contatti:
BDO Law S.r.l. Sta

Milano
Viale Abruzzi, 94