

NIS2 E DORA: CONFRONTO E CONVERGENZA

AUTORE: **Elena Maderna**

Data Protection Manager – Gruppo San Donato



Milano, maggio 2025

Panorama Normativo Europeo in Evoluzione

L'UE rafforza le politiche di sicurezza informatica e resilienza digitale

Normative chiave

- **NIS 2** - per i settori strategici
- **DORA** - per il settore finanziario

Obiettivi comuni

- Rafforzare la **resilienza operativa**
- Proteggere le **infrastrutture critiche**
- Armonizzare le **risposte agli incidenti ICT**

Direttiva (UE) 2022/2555 – D.Lgs. 138/2024 (Italia)

Obiettivo: Rafforzare la cybersecurity nei settori pubblico e privato

Obblighi principali:

- Adozione di **misure di gestione del rischio**
- **Notifica** e **reporting** degli incidenti significativi
- **Verifiche ispettive** e obbligo di conformità normativa

Ambito di applicazione:

- Estesa a **18 settori strategici**, tra cui:
- Energia, Sanità, Trasporti, Servizi Bancari, ICT, Pubblica Amministrazione, Settore Spaziale

Focus specifico:

- Maggiore attenzione alla **supply chain ICT** e ai **fornitori critici**

Classificazione e criteri applicativi

Soggetti Essenziali

- Settori ad **alta criticità**
- **Imprese con oltre 250 dipendenti e fatturato > €50M oppure bilancio > €43M**
- Include:
 - **PA centrali**
 - **Gestori DNS**
 - **Fornitori di reti pubbliche**

Soggetti Importanti

- Organizzazioni di media dimensione (50–250 dipendenti)
- Operanti in settori meno critici o in ambito ICT strategico

Nota

- Obblighi estesi anche ai **prestatori di servizi digitali, indipendentemente dalle dimensioni**

Innovazioni normative di rilievo:

Responsabilità diretta

- Coinvolgimento esplicito dei **vertici aziendali** nella gestione della cybersecurity

Nuovi poteri per le autorità competenti

- Ispezioni mirate
- Vulnerability scan
- Audit di sicurezza

Sanzioni elevate

- Fino a **€10 milioni** o **2% del fatturato globale annuo**, a seconda del valore più alto

Obblighi di notifica all'ACN

- **Avviso iniziale:** entro **24 ore**
- **Aggiornamento:** entro **72 ore**
- **Rapporto finale:** entro **1 mese**

Digital Operational Resilience Act(DORA)

Regolamento (UE) 2022/2554

Entrata in vigore: 17 gennaio 2025.

Obiettivo

- Garantire la **resilienza operativa digitale** del settore finanziario europeo.

Armonizzazione normativa:

- Supera le **discrepanze tra Stati Membri**
- Regolamento = **direttamente applicabile** in tutti i Paesi UE (senza recepimento nazionale)

Ambito esteso e soggetti coinvolti:

Istituzioni finanziarie

- Banche
- Assicurazioni
- SGR (Società di Gestione del Risparmio)
- SIM (Società di Intermediazione Mobiliare)
- Istituti di pagamento e di moneta elettronica

Altri soggetti rilevanti

- Fintech
- Gestori di asset digitali
- Piattaforme di crowdfunding
- Fornitori ICT critici

Monitoraggio diretto

- I **fornitori ICT critici** saranno supervisionati direttamente dalle **autorità europee di vigilanza (ESAs)**

Requisiti operativi e gestionali:

Gestione del rischio ICT

- Risk management ICT strutturato e documentato

Piani operativi

- Piani di continuità operativa (BCP)
- Piani di disaster recovery (DRP)

Testing periodico

- Stress test
- Penetration test
- Simulazioni di scenari

Contratti con fornitori ICT

- Clausole obbligatorie di sicurezza e auditabilità
- Mappatura delle dipendenze operative da terze parti critiche

Poteri delle ESAs

- Possibilità di imporre multe e sospensioni contrattuali in caso di non conformità

DIFFERENZE TRA NIS 2 E DORA

CARATTERISTICA	NIS 2	DORA
Tipo normativa	Direttiva (recepimento nazionale)	Regolamento (effetto diretto)
Settori coinvolti	18 settori strategici (es. PA, energia, sanità)	Settore finanziario e fornitori ICT
Obblighi	Cybersecurity e notifiche incidenti	Resilienza operativa ICT, notifica incidenti
Entrata in vigore	In vigore dal 2024	17 gennaio 2025
Sanzioni	Fino a €10M / 2% fatturato	Severe, anche per fornitori

Come adeguarsi a NIS 2 e DORA:

Inventario degli asset IT

- Rilevazione completa di sistemi, dati, reti, fornitori e infrastrutture

Cyber hygiene & formazione continua

- Campagne di awareness
- Gestione sicura delle credenziali
- Simulazioni phishing regolari

Gestione vulnerabilità

- Vulnerability assessment
- Patching ciclico
- Penetration testing periodici

Incident detection & response

- Implementazione di SIEM (Security Information and Event Management)
- Creazione di SOC (Security Operations Center), team IR (Incident Response), playbook e runbook per la gestione delle crisi

Risk management & fornitori

- BIA (Business Impact Analysis), BCP (Business Continuity Plan) / DRP (Disaster Recovery Plan)
- Valutazione del rischio delle terze parti
- Contratti conformi con i fornitori ICT

CONVERGENZA TRA NIS2, DORA E GDPR

Approccio integrato per le organizzazioni soggette a più normative:

Entità soggette

- Alcune organizzazioni (es. **banche sistemiche o grandi fornitori ICT**) sono soggette contemporaneamente a **NIS 2, DORA e GDPR**

Punti di convergenza

- **Notifica e gestione degli incidenti**
 - Obbligo di notificare gli incidenti rilevanti entro **tempi stringenti**
 - **GDPR**: entro **72h**
 - **NIS 2**: entro **24-72h**
 - **DORA**: tempistiche **definite dalle ESAs e BOI**
- Necessità di un **framework comune** per **detection, escalation e reporting**

Governance e responsabilità

- Responsabilità **diretta del top management** sulla sicurezza informatica, resilienza operativa e protezione dei dati, come richiesto da tutti e tre i regolamenti

Valutazione e gestione del rischio:

Valutazione del rischio

- GDPR: DPIA (Data Protection Impact Assessment) per trattamenti ad alto rischio
- DORA/NIS 2: Risk assessment ICT e piani di continuità operativa (BCP/DRP)

Controllo su fornitori e terze parti

- Obbligo di auditabilità
- Clausole contrattuali di sicurezza
- Gestione del rischio supply chain in tutti i framework

Formazione e sensibilizzazione del personale

- Obbligo di awareness e training continuo su minacce, compliance e policy aziendali

Audit e documentazione

- Tracciabilità delle attività: log, controlli di sicurezza
- Registro trattamenti (GDPR), audit trail ICT (DORA/NIS 2)

Integrazione dei requisiti

- Framework condivisi (es. ISO/IEC 27001, NIST, ENISA)
- Semplifica la compliance multi-normativa e le ispezioni

CONVERGENZA TRA NIS2, DORA E GDPR

Comunicazione di gravi incidenti ICT e delle minacce informatiche significative

Regolamento UE 2022/2554 - Resilienza operativa digitale per il settore finanziario (DORA)

Condividi    

A partire dal 17/01/2025 - data di applicazione del regolamento UE 2022/2554 (DORA) - le entità finanziarie di cui all'articolo 2 dello stesso regolamento sono tenute a segnalare **alla Banca d'Italia tutti i gravi incidenti ICT** e, su base volontaria, le minacce informatiche significative. In aggiunta, per le banche, gli istituti di pagamento, i prestatori di servizi di informazione sui conti e gli istituti di moneta elettronica gli obblighi segnaletici si estendono anche agli incidenti operativi o relativi alla sicurezza dei pagamenti che li riguardano.

Le segnalazioni dovranno essere effettuate tramite la piattaforma INFOSTAT della Banca d'Italia.

Per agevolare gli operatori nella raccolta e rappresentazione delle informazioni da comunicare, ai sensi del Regolamento DORA e dei relativi atti delegati, sono fornite in questa pagina le istruzioni operative per la segnalazione e la necessaria modulistica.

Si precisa che le informazioni qui contenute si applicano ai seguenti soggetti vigilati: banche, imprese di investimento, gestori, istituti di pagamento, istituti di moneta elettronica, emittenti di token collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di crowdfunding.

Sempre a decorrere dal 17 gennaio 2025, l'[attuale quadro di segnalazione](#) dei gravi incidenti operativi o di sicurezza applicato a banche, IP e IMEL si intenderà abrogato e sostituito da quello qui descritto.

CONVERGENZA TRA NIS2, DORA E GDPR

[Agenzia](#) ▾ [PNRR](#) [NIS](#) ▾ [Cloud](#) ▾ [CSIRT Italia](#) ▾ [NCC Italia](#) ▾ [Lavora con noi](#)



Argomenti

[Strategia Nazionale](#)

[Cybersicurezza](#)

p>Il Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, Roberto Baldoni, e il Direttore Generale della Banca d'Italia, Luigi Federico Signorini, hanno firmato oggi un protocollo d'intesa per lo scambio informativo e la collaborazione in materia di sicurezza cyber.

In particolare, l'ACN e la Banca d'Italia scambieranno informazioni idonee a prevenire e contrastare incidenti cyber che, anche potenzialmente, possano riguardare gli ambiti di interesse di ciascuna Istituzione. Inoltre, la collaborazione permetterà lo scambio di report informativi riferiti a tecniche, tattiche e procedure di attacco o tecnologie di prevenzione e protezione dalle minacce cyber.

- [acn_guida_notifica_incidenti_clear-pdf](#)

CONVERGENZA TRA NIS2, DORA E GDPR

2.18 I soggetti DORA (Regolamento 2022/2554) devono adempiere agli obblighi previsti dalla nuova disciplina NIS ?



DORA (Regolamento 2022/2554) è considerata lex specialis settoriale per la maggior parte delle previsioni della Direttiva NIS (2022/2555).

Pertanto, ai soggetti DORA riconducibili alle medie o grandi imprese e che svolgono attività o erogano servizi riconducibili alle tipologie di soggetto di cui all'allegato I, punti 3 (settore bancario) e 4 (settore infrastrutture dei mercati finanziari), **si applicano solamente le disposizioni del decreto NIS relative all'obbligo di registrazione (articolo 7, comma 1, del decreto NIS).**

In sostanza, l'articolo 3, comma 14, si limita a disapplicare, per tali soggetti, solo le previsioni dell'articolo 17 e dei capi IV e V, fermo restando il ruolo di CyCLONe nel contesto della gestione delle crisi cyber a livello transfrontaliero.

Obblighi significativi = opportunità di maturazione digitale

- La conformità alle normative come leva per il miglioramento e l'evoluzione digitale

Protezione di reputazione, clienti e continuità

- La compliance non è solo un obbligo, ma una misura di **protezione e fiducia** per l'azienda

Impegno strategico richiesto

- Coinvolgimento del **top management**, budget **dedicato**, e **roadmap pluriennale** per la gestione della conformità

Un ecosistema digitale resiliente = vantaggio competitivo

- La resilienza operativa digitale come **driver di competitività** nel mercato





CONSILIA BUSINESS MANAGEMENT S.r.l.

• Corso Europa, 13 – 20122 Milano

• **TEL:** +39 02 873 89 370 | **Fax:** +39 02 873 89 371

• **Sito web:** www.consiliabm.com

• **MAIL:** segreteria@consiliabm.com

info@consiliabm.com