LaScala formazione IMPRESA SOCIALE

Per ASSIFACT Associazione Italiana per il Factoring

Regolamento DORA

Framework normativo e impatto sul sistema finanziario UE

Avv. **Margherita Domenegotti**
Partner La Scala Società tra Avvocati

Avv. **Francesco Concio**
Partner La Scala Società tra Avvocati

27 marzo 2025

Il regolamento DORA

Che cos'è il Regolamento DORA?

Il Digital Operational Resilience Act, o DORA, è un regolamento dell'Unione Europea (UE) 2022/25541 che **stabilisce un *framework* vincolante e completo relativo alla gestione del rischio delle tecnologie di informazione e comunicazione (ICT) per il settore finanziario dell'UE.**

Quale contesto europeo?

Il Regolamento è parte del "Pacchetto UE sulla finanza digitale" lanciato nel settembre 2020, che include anche la Digital Finance Strategy, il Regolamento sui Mercati di Cripto-Asset (MICA) e un regime pilota sulle infrastrutture di mercato basate sulla Distributed Ledger Technology (DLT), introdotto dal Regolamento UE 2022/858.

A quali soggetti si applica?

Entrato in vigore 16 gennaio 2023 e applicabile dal 17 gennaio 2025, il testo normativo si applica non solo alle istituzioni finanziarie tradizionali, come banche, società di investimento e istituti di credito, e ai loro fornitori di servizi ICT critici di terze parti, ma anche ad alcune realtà emergenti nel settore finanziario, come i fornitori di servizi di cripto-asset (CASP), i fornitori di servizi di crowdfunding e i gestori di fondi di investimento alternativi (GEFIA).

DORA: la *timeline* del framework normativo

DORA mira a favorire l'armonizzazione dei requisiti di resilienza digitale per il settore finanziario europeo

GENNAIO 2023
ENTRA IN VIGORE IL REGOLAMENTO DORA

GIUGNO 2024
NORMATIVA DI II LIVELLO - I BATCH

RTS relativi a:

1. **criteri di classificazione degli incidenti;**
2. **gestione del rischio;**
3. **policy per l'uso di servizi ICT.**

In attesa di pubblicazione in Gazzetta UE dei Final Report sugli ulteriori RTS richiesti da DORA

LUGLIO 2024
NORMATIVA DI II LIVELLO - II BATCH

GENNAIO 2025
IL REGOLAMENTO DORA DIVIENE PIENAMENTE APPLICABILE

Le realtà del settore finanziario sono tenute al rispetto del DORA, che introduce importanti novità sul fronte della sicurezza

DORA: i cinque pilastri fondamentali

1. **Requisiti per la governance e la gestione dei rischi ICT**, fondati su principi chiave e norme comuni stabilite dalle Autorità Europee di Vigilanza Finanziaria (AEV), applicabili alle istituzioni finanziarie, tenendo conto del principio di proporzionalità.
2. **Obblighi di segnalazione degli incidenti ICT significativi**, con criteri, modelli e meccanismi uniformi e semplificati.
3. **Test di resilienza operativa digitale** per aggiornare e verificare regolarmente i sistemi e le procedure di risposta a cyber attacchi o interruzioni ICT, garantendo così la resilienza operativa.
4. **Gestione dei rischi legati ai fornitori terzi di servizi ICT** per le entità finanziarie, con l'introduzione di requisiti di gestione dei rischi e un quadro di sorveglianza diretta per i fornitori critici di servizi ICT.
5. **Condivisione delle informazioni** tra le autorità competenti.

DORA: il ruolo centrale delle ESAS

Il Regolamento DORA attribuisce alle Autorità di vigilanza europee, le ESAs, un ruolo centrale per assicurare una corretta applicazione della normativa, riconoscendo loro una serie di competenze specifiche.

Attività tecnico-regolamentare di II livello

Preparazione di:

- **Standard Tecnici Regolatori (RTS);**
- **Standard Tecnici di Implementazione (ITS)**
- **Linee guida o rapporti**.

Diventano vincolanti con l'adozione da parte della Commissione Europea di regolamenti delegati.

I Regolamenti adottati nel 2025:

1) Regolamento (UE) 2025/295 - Norme tecniche di regolamentazione (RTS)
2) Regolamento (UE) 2025/301- Notifica obbligatoria di incidenti gravi ICT;
3) Regolamento (UE) 2025/420 - Norme per la composizione del gruppo di esaminatori congiunto ESAs per la sorveglianza sui fornitori terzi critici di servizi ITC.

Hub unico per la segnalazione degli incidenti ICT significativi (art. 21 DORA)

Rapporto di analisi di tre modelli di gestione delle segnalazioni, con livelli crescenti di centralizzazione:

- **Scenario di base:** le entità finanziarie segnalano gli incidenti alle autorità nazionali, che a loro volta trasmettono le informazioni alle ESAs e ad altri enti competenti;
- **Modello di condivisione dati:** caricamento delle segnalazioni su una piattaforma comune centralizzata, consultabile da tutte le autorità competenti europee e nazionali;
- **Modello completamente centralizzato:** segnalazione degli incidenti a un Hub dell'UE, accessibile senza passare attraverso le autorità nazionali.

DORA: i rapporti con la Direttiva NIS 2

Parte I

Che cos'è la Direttiva NIS 2 ?

La **Direttiva NIS 2** è la seconda versione della Direttiva Europea per la sicurezza delle reti e dei sistemi informativi (NIS 1), pensata per migliorare la resilienza informatica delle aziende, entrata in vigore il 16 ottobre 2024.

Quali gli obiettivi

Garantire un livello più elevato di protezione, una risposta più efficace agli incidenti informatici e una maggiore cooperazione tra gli Stati membri.

Ambito di applicazione

I destinatari della normativa NIS 2 si identificano in base a **tre criteri cumulativi**, salvo che il soggetto non venga classificato come essenziale/importante dallo Stato stesso.

1 Requisito territoriale

Ai soggetti che svolgono i propri servizi o svolgono le proprie attività all'interno dell'Unione all'interno dell'Unione Europea.

2 Requisito dimensionale

Medie o grandi imprese ai sensi della Raccomandazione (CE) 2003/361:

- ❑ occupano più di 50 dipendenti;
- ❑ superano un fatturato annuo di € 50 milioni, o un totale di bilancio annuo di € 43 milioni.

3 Requisito settoriale

Ai soggetti che appartengono a settori economici

ESSENZIALI:

- ❑ **Bancario e finanziario**
- ❑ **Pubbliche amministrazioni**
- ❑ **Sanitario**
- ❑ **Trasporti**
- ❑ **Infrastrutture digitali**
- ❑ **ICT service management (B2B)**
- ❑ **Acqua potabile e rifiuti**
- ❑ **Sanitario**
- ❑ **Energia**

IMPORTANTI:

- ❑ **Servizi postali**
- ❑ **Gestione dei rifiuti**
- ❑ **Produzione e distribuzione di prodotti chimici**
- ❑ **Grande distribuzione**
- ❑ **Manifatturiero (con specifico riferimento ai dispositivi medici e prodotti elettronici)**
- ❑ **Servizi digitali**
- ❑ **Ricerca scientifica**

DORA: i rapporti con la Direttiva NIS 2

Parte II

La Direttiva prevede **controlli di sicurezza** rigorosi che devono essere formalizzati. In particolare, le aziende sono tenute a:

Avere una **governance** adeguata

Adottare procedure di **gestione del rischio**

Prevedere specifiche **clausole contrattuali sulla cyber sicurezza**, rinegoziando i contratti con i fornitori di servizi ICT

Notificare prontamente gli attacchi informatici alle autorità competenti. ICT

In che rapporti si pone il Regolamento DORA con la Direttiva NIS 2?

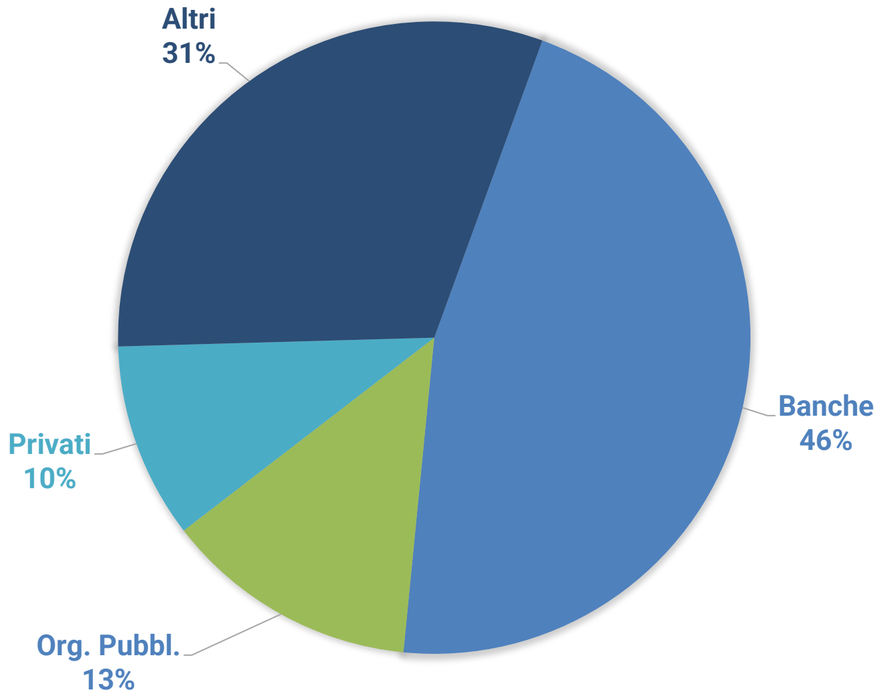
Il Considerando 28 della Direttiva NIS 2 riconosce che il Regolamento DORA deve essere considerato un atto giuridico specifico per il settore finanziario, una ***lex specialis***.

Trend e prospettive nel sistema finanziario UE

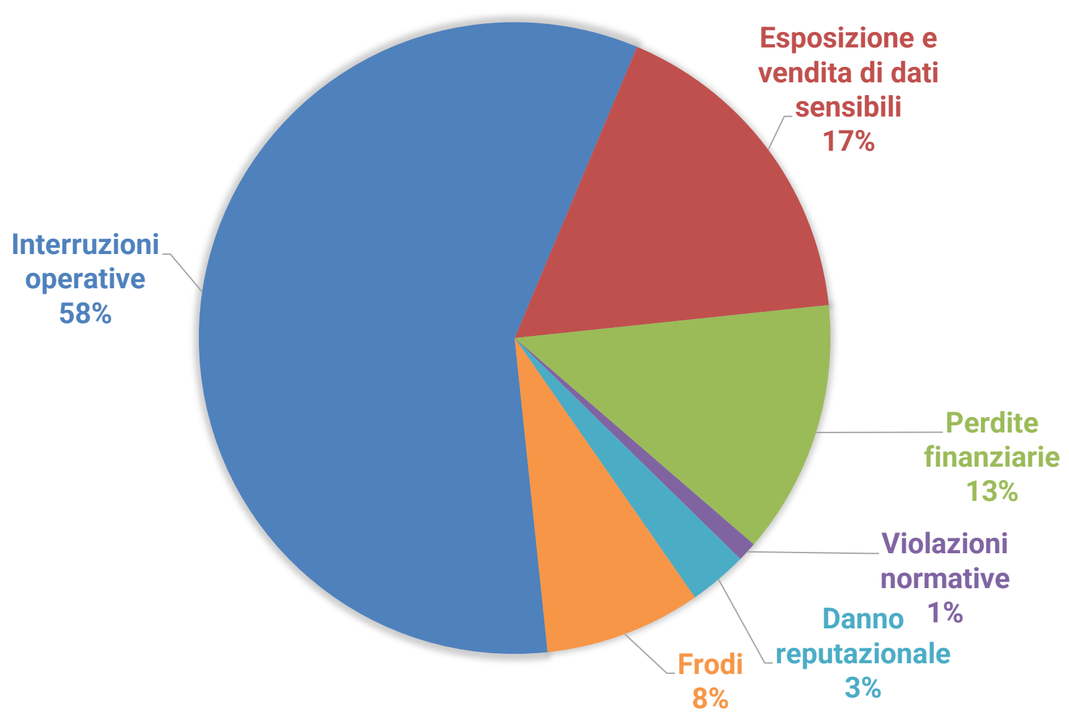
"*ENISA THREAT LANDSCAPE: FINANCE SECTOR*" di ENISA (Agenzia per la cybersicurezza dell'Unione Europea)

Prima analisi sul panorama delle minacce informatiche del settore finanziario europeo (gennaio 2023 - giugno 2024), pubblicato il 21 febbraio 2025, avente ad oggetto ben **488 incidenti**.

CATEGORIE



NATURA DELLE CONSEGUENZE



La normativa interna: a) il Decreto Legislativo 10 marzo 2025, n. 23

Pubblicato in Gazzetta Ufficiale n. 58 dell'11 marzo 2025, è il **primo intervento normativo per l'adeguamento della normativa nazionale al Regolamento (UE) 2022/2554 (DORA)** e rafforza le autorità di vigilanza e disciplina gli obblighi per operatori finanziari e fornitori di servizi ICT, anche attraverso la modifica di TUB e TUF.

Art. 1 / Art. 2

Individuazione delle "Autorità competenti DORA" (Banca d'Italia, Consob, IVASS, COVIP) e dell'Autorità nazionale competente NIS (Agenzia per la cybersicurezza nazionale e CSIRT Italia) **[art.1]**; definizione dell'ambito di applicazione, includendo intermediari finanziari e Bancoposta, senza interferenza con le norme sulla sicurezza cibernetica nazionale (DL n. 105/2019) **[art.2].**

Art. 3 / Art. 4 / Art. 5

Definizione delle competenze delle Autorità nazionali e modalità di partecipazione al «forum di sorveglianza» **[art.3];** indicazione della disciplina delle segnalazioni di gravi incidenti TIC e della notifica volontaria delle minacce informatiche **[art.4];** precisazione della necessaria cooperazione tra le Autorità competenti tramite Protocolli d'intesa per garantire il coordinamento informativo e operativo **[art.5].**

Art. 6 / Art. 7

Previsione di un framework semplificato per la gestione dei rischi ICT in relazione agli intermediari finanziari minori, lasciando alla Banca d'Italia l'identificazione di quelli «significativi» **[art.6];** prescrizione anche a Bancoposta di adottare il *framework* completo di gestione dei rischi ICT **[art.7].**

Focus: il regime sanzionatorio

Il Decreto Legislativo prevede **un regime sanzionatorio chiaro e differenziato** per la mancata osservanza delle norme DORA, garantendo l'efficacia nell'applicazione del regolamento attraverso l'attribuzione alle Autorità interne di ampi poteri

Poteri ispettivi

Le Autorità interne, presso i terzi fornitori di servizi ICT hanno le seguenti facoltà:

- ❑ convocare gli amministratori e il personale;
- ❑ Richiedere documenti e informazioni;
- ❑ Esercitare i poteri già previsti dalla legislazione bancaria, finanziaria e assicurativa [art.8]

Poteri regolamentari

Le Autorità interne possono emettere disposizioni attuative in linea con gli orientamenti delle Autorità europee di vigilanza, assicurando un'applicazione uniforme della disciplina [art.9]

Poteri sanzionatori

Le Autorità interne possono comminare sanzioni per:

- ❑ violazione del Regolamento DORA e delle norme di regolamentazione e attuazione;
- ❑ mancata collaborazione o il mancato seguito dato alle indagini, ispezioni o richieste previste dall'art. 8

Focus: art. 10 "*Sanzioni amministrative e altre misure*"

Sanzioni amministrative pecuniarie

Sanzioni amministrative pecuniarie - persone giuridiche

- Le sanzioni vanno da € 30.000 fino a raggiungere il 10% del fatturato per banche e intermediari finanziari, da € 30.000 a fino a € 3,5 milioni ovvero fino al 7% del fatturato per assicurazioni e fondi pensione e da € 30.000 fino a € 5 milioni o il 10% del fatturato per i fornitori di servizi ICT critici. Nel caso dei depositari centrali di titoli e dei relativi fornitori di servizi TIC, in caso di sanzioni gravi, il minimo edittale rimane 30mila euro, mentre il massimo è di 20 milioni o il 10% del fatturato, qualora sia superiore.

Sanzioni amministrative pecuniarie - persone fisiche

- i «*soggetti apicali*» ossia le persone fisiche "*che svolgono funzioni di amministrazione, direzione o controllo e del personale delle società e degli enti nei confronti dei quali sono accertate le violazioni*", quando l'inosservanza è conseguenza della violazione dei doveri propri o dell'organo di appartenenza e la condotta ha inciso sull'organizzazione o sui profili di rischio aziendali o ha contribuito a determinare la violazione da parte dell'ente" (importi da "**5.000 euro a 5 milioni,** in caso di condotte più gravi o **fino a 3,5 milioni in caso di condotte meno gravi")**.

Misure accessorie interdittive

Da un minimo di 6 mesi ad un massimo 3 anni di interdizione dallo svolgimento di attività

Responsabilità penale

«*Salvo che il fatto costituisca reato* […]»,

DORA: procedure di allineamento

Gli enti coinvolti devono prepararsi al DORA non solo mediante un'analisi delle misure tecniche, ma anche attraverso attività di compliance, che prevede i seguenti step:

Analisi strutturale

Revisione della struttura interna e delle misure di sicurezza eventualmente già adottate

Reportistica

Valutazione della capacità di reporting dell’ente, implementazione o revisione delle procedure di segnalazione dei cyberattacchi

Monitoraggio fornitori ICT

Mappatura dei contratti con i fornitori terzi di servizi ICT e valutazione del grado di criticità ed eventuale rinegoziazione degli obblighi contrattuali

La normativa interna: b) le comunicazioni di Banca d'Italia

Obiettivo generale:
rafforzamento della responsabilità degli intermediari e stimolo a un approccio proattivo nella gestione dei rischi digitali

1° 23.12.2024	Richiesta di autovalutazione ai soggetti vigilati su gestione dei rischi ICT, strategie di terze parti, contratti di fornitura e test di resilienza. Obiettivo: maggiore trasparenza e solidità nella gestione dei rischi.
2° 30.12.2024	Chiarimenti su: struttura della funzione di controllo ICT; comunicazione dei contratti con fornitori ICT; segnalazione di incidenti ICT e minacce informatiche; Test avanzati di penetrazione (TLPT).
3° 13.02.2025	Istruzioni operative sulla sicurezza ICT e modello per la autovalutazione, con scadenza al 30 aprile 2025.
4° 14.03.2025	Tempistiche per la trasmissione dei registri sugli accordi contrattuali con i fornitori ITC, il successivo controllo che effettuerà sugli stessi e le ulteriori attività di verifica ad opera delle ESAs.

DORA: la roadmap di adeguamento in materia ICT

«*Tabella di marcia*» verso la creazione di un sistema integrato di sicurezza in armonia con la normativa di settore

Invio alle ESAs dei registri informativi sugli accordi con i fornitori terzi di servizi ICT ricevuti dalle entità finanziarie

entro aprile 2025

I fornitori potranno presentare una dichiarazione motivata e le relative informazioni di supporto per opporsi alla valutazione

entro sei settimane

***roadmap* 2025: designazione dei fornitori terzi di servizi ICT critici (CTPP)**

entro luglio 2025

Le ESAs condurranno le valutazioni di criticità previste dal Regolamento DORA e notificheranno ai fornitori di servizi ICT di terze parti se sono stati classificati come critici

ulteriori 6 settimane

Le ESAs designeranno i fornitori critici e avvieranno il processo di supervisione. I fornitori non designati potranno volontariamente richiedere di essere inclusi nell'elenco

Considerazioni finali

La disciplina DORA è destinata ad assumere sempre maggior rilevanza nel dibattito quotidiano sull'importanza della resilienza digitale e della *cybersecurity*.

Il **Decreto legislativo n. 23 del 10 marzo 2025** segna un momento decisivo per il settore finanziario italiano, rafforzando le misure di sicurezza informatica e allineando il nostro sistema alle disposizioni europee.

In che modo?

REGOLE DEFINITE

Quadro di regole più chiaro, poteri ispettivi ampliati e un regime sanzionatorio articolato

APPROCCIO STRUTTURATO

Approccio strutturato alla gestione del rischio digitale, per garantire una maggiore resilienza dell'intero comparto.

COLLABORAZIONE

Con le istituzioni e le autorità deputate al controllo delle innovative misure di settore

LaScala formazione
IMPRESA SOCIALE

Grazie per l'attenzione

Avv. Margherita Domenegotti
Partner La Scala
m.domenegotti@lascalaw.com

Avv. Francesco Concio
Partner La Scala
f.concio@lascalaw.com

LA SCALA FORMAZIONE

info@lascalaformazione.com

+39 378 3054263

Sede legale:
Via Correggio, 43
Milano