DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Implementazione DORA: autorità competenti e quadro sanzionatorio

10 Giugno 2025

Savino Casamassima, Partner, Qubit Law Firm & Partners
Massimiliano Nicotra, Partner, Qubit Law Firm & Partners

Savino Casamassima, Partner, Qubit Law Firm & Partners

Massimiliano Nicotra, Partner, Qubit Law Firm & Partners

Savino Casamassima

Savino Casamassima è un Avvocato del Foro di Milano. Ha una significativa esperienza presso studi legali italiani ed internazionali a Milano e Londra ed ha ricoperto funzioni apicali in ambito sia legale che compliance presso banche internazionali e società operanti nel mondo dei servizi bancari e fintech. Già membro di Consigli di Amministrazione ed Organismi di Vigilanza 231 presso banche ed intermediari finanziari internazionali.

Massimiliano Nicotra

Massimiliano Nicotra è avvocato e si occupa di diritto della tecnologia da oltre vent'anni. E' Data Protection Officer di società multinazionali. Coordinatore della sezione Privacy e Compliance del Centro di Ricerca Economica e Giuridica nonché Vicepresidente del Comitato Strategico del Centro di Ricerca sull'Amministrazione Digitale presso l'Università degli Studi di Roma Tor Vergata.

1. Premessa: il D. Lgs. 23/2025 ed il coordinamento con la normativa EU DORA

Il Regolamento (UE) 2022/2554 ("**DORA**" – Digital Operational Resilience Act) ha introdotto un quadro normativo uniforme sulla resilienza operativa digitale per il settore finanziario in tutta l'Unione Europea. Entrato in vigore il 17 gennaio 2025, DORA impone requisiti armonizzati in materia di gestione dei rischi ICT, segnalazione di incidenti informatici e sorveglianza sui fornitori terzi di servizi tecnologici per gli enti finanziari. Per garantire l'effettiva applicazione di DORA a livello nazionale, l'Italia ha adottato il **Decreto Legislativo 10 marzo 2025, n. 23**, pubblicato in Gazzetta Ufficiale l'11 marzo 2025, adeguando l'ordinamento interno ai dettami del DORA e recependo la correlata direttiva (UE) 2022/2556.

Il D.Lgs. 23/2025 si inserisce dunque in un quadro normativo in evoluzione, interagendo sia con la disciplina europea sia con quella nazionale previgente in cui, tra l'altro, l'Italia ha di recente recepito anche la direttiva NIS 2 (D.Lgs. 21 settembre 2024, n. 138) per la cybersecurity nei settori critici. Il decreto DORA coordina tali ambiti, evitando sovrapposizioni: ad esempio, chiarisce e coordina il ruolo dell'**Agenzia per la Cybersicurezza Nazionale** (ACN) – autorità NIS – con riferimento alle previsioni regolamentari ed integra le definizioni NIS2 nel proprio testo. Inoltre, attraverso il recepimento della direttiva (UE) 2022/2556, sono state modificate le normative di settore (TUB, TUF, Codice Assicurazioni, ecc.) per allinearle a DORA, inserendo espliciti riferimenti alla resilienza operativa digitale.

Si procederà nel seguito ad esaminare in dettaglio le previsioni del D.Lgs. 23/2025, con particolare riferimento alle **autorità competenti** designate in ambito DORA in Italia ed al regime delle **sanzioni**, con alcune considerazioni conclusive sulle sfide applicative di questa riforma.

2. L'individuazione delle autorità competenti DORA a livello italiano

Il Regolamento DORA richiede agli Stati membri di designare le **autorità competenti** incaricate di assicurare che le varie categorie di entità finanziarie rispettino i requisiti della resilienza operativa digitale (artt. 46-47 DORA). L'art. 3 del D.Lgs. 23/2025 ha provveduto in tal senso, individuando le autorità nazionali competenti DORA e il loro ruolo a livello domestico ed europeo, come segue:

- **Banca d'Italia** – Autorità competente DORA per banche e gruppi bancari, istituti di pagamento, istituti di moneta elettronica, società capogruppo di gruppi finanziari, controparti centrali

vedi l'articolo online

(CCP), sedi di negoziazione all'ingrosso di titoli di Stato e, più in generale, per tutti i soggetti vigilati da Banca d'Italia ai sensi del Testo Unico Bancario (TUB). Inoltre, come precisato dal comma 2 dell'art. 3, Banca d'Italia è l'autorità competente per **Cassa Depositi e Prestiti S.p.A.** (data la natura peculiare di tale ente). Il comma 3 ne estende la competenza anche agli **intermediari finanziari non bancari iscritti ex art. 106 TUB** e ai servizi di **Bancoposta**.

- **Consob** – Autorità competente DORA per le entità vigilate in ambito mercati finanziari e servizi d'investimento. In particolare, rientrano nella competenza Consob le **imprese di investimento** (SIM), le **società di gestione del risparmio** (SGR) e le altre entità di mercato indicate nell'art. 2, par.1, lett. g) e i) DORA (ad esempio, sedi di negoziazione diverse da quelle all'ingrosso dei titoli di Stato, sistemi di scambio, data reporting services). Consob, in sintesi, copre gli obblighi DORA per i soggetti già sottoposti alla sua vigilanza ai sensi del TUF.

- **IVASS** – Autorità competente DORA per il settore assicurativo. Sono attribuiti a IVASS i poteri di vigilanza DORA verso le **imprese di assicurazione e di riassicurazione**, ossia le entità finanziarie di cui alle lett. n) e o) dell'art. 2(1) DORA, corrispondenti alle compagnie assicurative e riassicurative disciplinate dal Codice delle Assicurazioni Private (CAP).

- **COVIP** – Autorità competente DORA per il settore previdenziale complementare. La COVIP sovrintende al rispetto degli obblighi DORA da parte dei **fondi pensione** e forme pensionistiche complementari (lett. p) dell'art. 2(1) DORA).

È importante notare che le autorità competenti agiscono "*secondo le rispettive attribuzioni di vigilanza*": ciò significa che ognuna interviene per i soggetti tradizionalmente di propria competenza. La scelta italiana risulta in linea con l'art. 46 DORA, che rinvia alle autorità settoriali già esistenti (es. autorità designate ai sensi di CRD IV/CRR per le banche, Solvency II per assicurazioni, ecc.).

La normativa DORA non menziona esplicitamente la **Banca Centrale Europea**, la quale tuttavia, nell'architettura della vigilanza bancaria, è l'autorità di vigilanza prudenziale per le banche "significative" nell'Eurozona. In pratica, per le banche significative DORA verrà attuata in coordinamento tra BCE e Banca d'Italia: quest'ultima rimane autorità competente nazionale DORA, ma la BCE, in virtù dei suoi poteri nel Meccanismo di Vigilanza Unico, potrà cooperare nell'assicurare il rispetto dei requisiti (ad esempio, integrando gli accertamenti DORA nelle proprie ispezioni SREP). Su questo aspetto, tuttavia, il decreto italiano non interviene direttamente (non potendo disciplinare le prerogative della BCE), limitandosi a designare la Banca d'Italia come referente nazionale.

È importante sottolineare che il D.Lgs. 23/2025 prevede che vengano adottati specifici protocolli tra le varie Autorità di vigilanza così designate, i quali dovranno coinvolgere anche ACN, al fine di agevolare lo scambio di informazioni, prevedere forme di consulenza ed assistenza reciproca e meccanismi di coordinamento per le fasi di *incident response*, ed il coordinamento sulle attività verso i soggetti essenziali ed importanti vigilati da ACN eventualmente designati come fornitori critici ai sensi del DORA.

3. Le sanzioni: contenuti

Un pilastro fondamentale di DORA è l'istituzione di un regime sanzionatorio efficace e dissuasivo per le violazioni degli obblighi di resilienza digitale. Il Regolamento UE fissa linee generali (ad es. prevede sanzioni amministrative fino a un massimo del **2% del fatturato annuo mondiale** per talune infrazioni, elevabile al **1% giornaliero nel caso di inadempienze continuative da parte di fornitori critici** – cfr. art. 34 DORA) e richiede, così come molti altri regolamenti europei, che siano previste dagli Stati membri sanzioni "*effettive, proporzionate e dissuasive*"). L'Italia, con l'art. 10 del D.Lgs. 23/2025, ha dato attuazione a tali previsioni inserendo nuove fattispecie sanzionatorie di natura amministrativa sia nel Testo Unico Bancario (TUB) sia nel TUF, nel Codice Assicurazioni e nel D.Lgs. 252/2005 (previdenza) per le rispettive categorie di enti.

Categorie di violazioni e importi edittali

Le sanzioni amministrative introdotte dal D.Lgs. 23/2025 sono di vario genere: oltre alle sanzioni pecuniarie, infatti, le Autorità di vigilanza possono adottare delle misure correttive nei confronti dei soggetti DORA (art. 50, comma 4 del Regolamento) che possono comprendere l'emissione di un ordine a non ripetere la violazione, la richiesta di cessazione temporanea di qualsiasi comportamento o pratica contraria alle previsioni regolamentari e, in generale, l'adozione di qualsiasi misura per far rispettare i requisiti.

Le sanzioni amministrative pecuniarie, a loro volta, variano **in base alla gravità della violazione** e **alla**

tipologia di soggetto coinvolto, secondo una struttura graduale. In generale, il decreto legislativo distingue due macro-classi di infrazioni DORA:

- **Violazioni "più gravi"** – tipicamente attinenti a obblighi di governance ICT, organizzazione e strategie, ruolo degli organi aziendali e responsabilità del management nella resilienza operativa (es. mancata istituzione di una funzione di gestione del rischio ICT, gravi carenze nel quadro di governance, omissione nella definizione del piano di continuità operativa, violazione dei doveri degli amministratori in materia ICT). Queste condotte sono sanzionate più severamente, con importi massimi più elevati.

- **Violazioni "meno gravi"** – riguardanti obblighi più operativi e procedurali, considerati di minore impatto. Vi rientrano, ad esempio, la **mancata classificazione corretta degli incidenti**, ritardi o omissioni formali nelle notifiche ed inadempienze minori rispetto ai requisiti di test periodici non critici.

Il D.Lgs. 23/2025 ha elencato specificamente quali articoli del Regolamento DORA ricadono in ciascuna categoria (inserendo tali elenchi negli articoli 144 e 144-ter TUB, e analogamente nelle norme di TUF/CAP). In pratica, tutto il "catalogo" degli obblighi DORA è sanzionato in caso di violazioni, ma con pesi diversi.

Perimetro soggettivo: le sanzioni per le entità giuridiche

Per gli **enti finanziari** e i **fornitori di servizi ICT** (persone giuridiche) le sanzioni pecuniarie previste dal decreto sono articolate come segue:

- **Enti vigilati finanziari (banche, istituti finanziari, ecc.): a) violazioni più gravi:** multa **da Euro 30.000 fino al 10% del fatturato annuo** dell'ente. Il minimo edittale è fisso (30mila euro), mentre il massimo è proporzionale al volume d'affari, senza tetto assoluto, salvo per alcuni casi particolari; b) **violazioni meno gravi:** multa **da Euro 30.000 fino al 7% del fatturato annuo**. Si riduce dunque il massimale per infrazioni ritenute di minore impatto (ma non il minimo edittale).

- **SIM, SGR e altri intermediari non bancari (ambito TUF): a) violazioni più gravi:** per le **Società di Intermediazione Mobiliare (SIM)**, **Società di Gestione del Risparmio (SGR)**, SICAV, SICAF, **controparti centrali (CCP)**, **gestori di mercati regolamentati** e i relativi fornitori ICT, il decreto ha fissato un tetto edittale *ibrido*: **da Euro 30.000 fino ad Euro 5.000.000**, oppure **fino al 10% del fatturato** se tale 10% eccede 5 milioni. In pratica, per queste entità il massimale di default è 5 milioni, ma se l'ente è molto grande, si applica il massimale proporzionale; b) **violazioni meno gravi: da Euro 30.000 fino a Euro 3.500.000**, oppure **fino al 7% del fatturato** se superiore a Euro 3,5 milioni. Analogamente a quanto sopra, la soglia fissa per infrazioni meno gravi nel settore TUF è 3,5 milioni, con possibilità di superarla se il 7% del fatturato eccede tale importo, mentre rimane fisso il minimo edittale.

- **Depositari centrali di titoli (CSD): a) violazioni più gravi:** per i **CSD** (ad es. Monte Titoli) e i loro fornitori ICT critici: multa **da Euro 30.000 fino a Euro 20.000.000**, oppure **fino al 10% del fatturato** se eccede Euro 20MM. Qui il massimale assoluto fisso sale a 20 milioni (dato il ruolo sistemico dei CSD), con eventuale adeguamento al 10% se più alto; b) per violazioni **meno gravi**, i CSD sono sanzionabili **da Euro 30.000 fino a Euro 14.000.000**, oppure **fino al 7% del fatturato** se eccede Euro 14MM.

- **Fornitori di servizi di crowdfunding: a) violazioni più gravi:** DORA si applica anche ai fornitori di servizi di crowdfunding regolamentati (Reg. EU 2020/1503). Per questi soggetti, tipicamente di piccole dimensioni, le sanzioni sono **da Euro 500 fino a Euro 500.000**, oppure **fino al 5% del fatturato** se eccede Euro 500k. Il limite percentuale del 5% riflette la minore criticità sistemica e i volumi ridotti di tali operatori; b) per violazioni **meno gravi** di crowdfunding: **Euro 500 fino a Euro 350.000**, oppure **fino al 3,5% del fatturato** se eccede Euro 350k.

- **Amministratori di indici di riferimento critici: a) violazioni più gravi:** Anche gli **amministratori di benchmark critici** (ad es. gli organismi tipo EURIBOR) rientrano in DORA. Le sanzioni per loro e relativi fornitori ICT: **Euro 10.000 fino a Euro 1.000.000**, oppure **fino al 10% del fatturato annuo** se eccede Euro 1M; b) per violazioni **meno gravi**: **Euro 10.000 fino a Euro 700.000**, oppure **fino al 7% del fatturato** se eccede Euro 700k.

Da notare che le *sanzioni pecuniarie* colpiscono anche i **fornitori terzi di servizi ICT** (in base alla catego-

ria del cliente servito): il decreto legislativo esplicitamente prevede che i provider tecnologici possano essere destinatari diretti di sanzioni amministrative. Ad esempio, un cloud provider qualificato come *"fornitore critico"* per le banche, se non rispetta gli obblighi derivanti dalla sua designazione (art. 28-30 DORA) o ostacola le ispezioni, potrà essere multato con gli importi previsti per la categoria banche. Tale estensione del perimetro soggettivo anche relativamente al sistema sanzionatorio costringe direttamente i soggetti che precedentemente non erano inclusi nella vigilanza di settore a rispettare la compliance DORA, pena conseguenze economiche significative e possibili interdizioni contrattuali.

Perimetro soggettivo: le sanzioni per persone fisiche

Oltre alle entità giuridiche, la normativa prevede sanzioni anche per gli **individui** responsabili delle violazioni, in particolare i componenti degli organi di amministrazione, direzione e controllo (*soggetti apicali*) e il personale coinvolto. Questa impostazione segue il modello già in vigore nel TUB (artt. 144-145) dove alle sanzioni agli enti si affiancano quelle a carico degli esponenti aziendali colpevoli.

Il D.Lgs. 23/2025, integrando l'art. 144-ter TUB, stabilisce che qualora l'inosservanza delle disposizioni del DORA sia conseguenza della violazione di doveri propri o dell'organo di appartenenza da parte di un soggetto apicale – e la condotta abbia inciso sull'assetto organizzativo o sui profili di rischio aziendali, contribuendo alla violazione dell'ente – tale soggetto è passibile di sanzione amministrativa pecuniaria. In pratica, se il Consiglio di Amministrazione o il dirigente responsabile ICT non adempie ai propri compiti (es. non approva il piano ICT, ignora le segnalazioni di rischio, non attua misure richieste) e ciò porta l'ente a violare DORA, scatta la punibilità personale.

Gli importi per le persone fisiche seguono anch'essi la distinzione tra casi più gravi e meno gravi:

- **Violazioni più gravi**: la sanzione per il soggetto apicale è compresa tra **Euro 5.000 fino ad Euro 5.000.000**. Questo intervallo vale per i casi collegati alle violazioni gravi compiute dall'ente nelle categorie principali (banche, SIM/SGR, CSD).

- **Violazioni meno gravi:** la sanzione al soggetto apicale e compresa tra **Euro 5.000 fino ad Euro 3.500.000**. Dunque, anche nelle infrazioni minori, il management può subire multe sostanziali, sebbene con un massimale ridotto.

- **Casi particolari – crowdfunding e indici critici:** per le violazioni imputabili a persone fisiche operanti presso fornitori di crowdfunding o amministratori di indici gli importi sono più bassi in ragione delle minori soglie previste per gli enti: rispettivamente **Euro 500 – Euro 500.000** (casi più gravi di crowdfunding) ed **Euro 500 – Euro 350.000** (casi meno gravi crowdfunding); **Euro 5.000 – Euro 500.000** (gravi indici critici) e **Euro 5.000 – Euro 350.000** (meno gravi indici critici).

È interessante notare come la fattispecie che integra la condotta passibile di sanzione sia abbastanza complessa, richiedendo la coesistenza di vari elementi. Innanzitutto, l'inosservanza della previsione DORA deve essere una conseguenza della violazione di doveri propri o dell'organo di appartenenza della persona fisica. Inoltre, la condotta posta in essere deve incidere in modo rilevante sulla complessiva organizzazione o sul profilo di rischio (o deve aver contribuito a determinare la mancata ottemperanza a un provvedimento dell'Autorità di vigilanza o alla mancata osservanza dell'ordine di porre termine a un comportamento in violazione).

Ciò significa che le sanzioni a carico delle persone fisiche **non sono automatiche** a ogni violazione dell'ente: deve sussistere appunto un **nesso di responsabilità diretta** e di **mancata diligenza** da parte dell'esponente, escludendo quindi una responsabilità oggettiva dell'organo di vertice, ma al contempo fissando criteri abbastanza ampi ("la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali …") che lasciano spazio all'azione punitiva qualora vi sia stata negligenza gestionale.

Le sanzioni accessorie

Le sanzioni accessorie costituiscono misure ulteriori che si aggiungono alle sanzioni principali (pecuniarie) per aumentarne l'efficacia deterrente o rimuovere situazioni di rischio. Nel contesto DORA la principale sanzione accessoria introdotta dal D.Lgs. 23/2025 è l'**interdizione temporanea dagli incarichi** a carico dei soggetti apicali responsabili (comma 2-quater art. 144-ter TUB). Altri possibili provvedimenti accessori possono essere, l'**Interdizione dagli uffici direttivi**, la **pubblicazione delle sanzioni**, **ordini e diffide correttive** da parte delle Autorità coinvolte oppure **misure nei confronti dei fornitori ICT**.

Tutte queste misure concorrono a creare un ecosistema di *enforcement* completo: non solo quindi la sanzione pecuniaria, ma l'interdizione e la pubblicità colpiscono la **reputazione e la carriera** dei re-

sponsabili, mentre le misure correttive tendono ad eliminare a monte il rischio di recidiva (costringendo l'ente a mettere in sicurezza i propri sistemi, pena ulteriori conseguenze).

In conclusione, le sanzioni accessorie previste dal regime italiano di attuazione DORA rafforzano significativamente il potere deterrente e ri-educativo dell'impianto sanzionatorio. Esse segnalano che l'obiettivo non è solo punire, ma soprattutto **prevenire il ripetersi** di incidenti gravi, rimuovendo eventuali cause umane (dirigenti inadeguati) o cause tecniche (fornitori inaffidabili). Dal punto di vista degli operatori, questo impone un ulteriore livello di attenzione: non basta gestire il rischio sanzione, ma bisogna dimostrare di aver messo in atto correttivi efficaci per poter continuare ad operare pienamente.

4. Conclusioni

L'implementazione italiana di DORA tramite il D.Lgs. 23/2025 rappresenta una svolta significativa nella regolamentazione finanziaria in materia di **cybersecurity e resilienza operativa**. Dal quadro emerso, possiamo trarre alcune considerazioni conclusive:

- **approccio organico e multidimensionale:** l'Italia ha adottato un approccio organico, inserendo DORA nel tessuto normativo esistente (TUB, TUF, CAP) e attivando sinergie sia verticali (tra livelli nazionale-europeo, es. partecipazione al forum di sorveglianza) sia orizzontali (tra autorità domestiche e con ACN). Questo approccio dovrebbe favorire un'attuazione coerente, evitando conflitti di competenza e doppioni.

- **severità del regime sanzionatorio:** l'apparato di sanzioni, con tetti fino al 10% del fatturato e milioni di euro anche per le persone fisiche è estremamente rigido e questo denota la serietà con cui si considera il rischio informatico. Ovviamente, l'effettività dipenderà da come le sanzioni verranno comminate: l'esperienza insegna che sanzioni troppo elevate in teoria potrebbero poi essere mitigate in concreto tenendo conto di attenuanti (cooperazione dell'ente, natura colposa vs dolosa, ecc.). DORA stesso prevede dei criteri di valutazione (art. 50(3) DORA: gravità, durata, grado di responsabilità, misure preventive adottate, ricorrenza, ecc.) per garantire un'applicazione equilibrata ed oggettiva delle stesse.

In conclusione, *cybersecurity* e *vigilanza finanziaria* oggi formano un binomio inscindibile: con DORA, i poteri di vigilanza e sanzione, tradizionalmente esercitati su patrimonio e trasparenza, si estendono alle reti, ai dati ed ai sistemi informativi. Si tratta di un cambio di paradigma che comporta oneri ma soprattutto opportunità di rafforzare la robustezza del nostro sistema bancario-finanziario. Le prime applicazioni pratiche diranno se l'impianto disegnato funziona a dovere: l'auspicio è che la combinazione di regole stringenti, cooperazione tra autorità e responsabilizzazione degli operatori contribuisca a ridurre significativamente il numero e l'impatto di incidenti informatici nel settore, a beneficio dell'intera collettività e della fiducia nei servizi finanziari digitali.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it