LCA

•ALERT•

7 LUGLIO 2023

Digital Operational Resilience Act

Le misure per tutelare il sistema finanziario dai rischi informatici

1. *FRAMEWORK* NORMATIVO

Come noto, il 27 dicembre 2022 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (*i.e., Digital Operational Resilience Act*) (c.d. "DORA" o "Regolamento").

La finalità del DORA è promuovere l'armonizzazione delle misure che gli enti finanziari devono adottare per innalzare la sicurezza dei propri sistemi digitali, tenuto conto della sempre più crescente esposizione del settore finanziario a rischi informatici.

Il DORA sarà in vigore a partire dal 17 gennaio 2025.

2. AMBITO APPLICATIVO DEL DORA

Il Regolamento si rivolge, tra l'altro, a un ampio novero di operatori del settore bancario, finanziario e assicurativo, nonché ai fornitori di servizi dell'informazione e della comunicazione ("ICT").

3. ADEMPIMENTI PRINCIPALI

Tra i numerosi adempimenti introdotti dalla nuova disciplina europea, gli operatori interessati dovranno:

- adottare un assetto di *governance* e organizzativo interno che garantisca un controllo efficace e prudente di tutti i rischi relativi alle ICT;
- predisporre un sistema per la gestione dei rischi informatici, creando un *ICT Risk Management Framework* e definendo una strategia di resilienza digitale;
- istituire procedure e processi appropriati per garantire, in maniera coerente e integrata, il monitoraggio e la gestione degli incidenti informatici, in un'ottica di prevenzione degli stessi, predisponendo altresì un sistema di segnalazione degli incidenti informatici da notificare alle Autorità competenti;
- svolgere dei "test di resilienza digitale" al fine di identificare punti deboli, carenze e lacune della resilienza operativa digitale e di attuare tempestivamente misure correttive;
- gestire i rischi informatici derivanti da terzi quali componenti integranti del proprio sistema di gestione dei rischi complessivi. Al riguardo, il DORA prevede che gli operatori regolino il rapporto commerciale con i fornitori ICT prevedendo, nei relativi accordi, specifiche previsioni contrattuali anche al fine di garantire un adeguato monitoraggio delle attività svolte da tali soggetti.

4. GLI *STANDARD* TECNICI

Al fine di agevolare gli operatori nel rispetto dei numerosi obblighi, il DORA prevede che le Autorità europee di vigilanza (c.d. ESAs) elaborino specifici *standard* tecnici.

In data 19 giugno 2023, le ESAs hanno avviato una consultazione pubblica su un primo gruppo di *standard* tecnici (*i.e.*, RTS e ITS) di attuazione del DORA, concernenti *inter alia* la gestione dei rischi ICT, nonché la classificazione degli incidenti connessi.

Le ESAs prevedono di presentare primi progetti di norme tecniche alla Commissione U.E. entro il 17 gennaio 2024.

5. IL *FRAMEWORK* DELLA *CYBER-SECURITY* E *OVER-REGULATION*

Il DORA si inserisce all'interno della nuova strategia dell'U.E. in materia di cybersicurezza che include la Direttiva (UE) 2016/1148 (di seguito, la "Direttiva NIS 1"), la futura Direttiva (UE) 2022/2555 (di seguito, la "Direttiva NIS 2") (la cui applicazione è prevista a decorrere dal 18 ottobre 2024), la Direttiva (UE) 2022/2557 (di seguito, la "Direttiva CER") (relativa alla resilienza dei soggetti critici), a cui si aggiunge - a livello domestico - la disciplina relativa al Perimetro di Sicurezza Nazionale Cibernetica.

Sia la Direttiva NIS 2 (destinata ad abrogare la Direttiva NIS 1) che la Direttiva CER mirano a garantire un livello elevato di cybersicurezza a livello U.E. e si applicheranno anche ai settori bancario e finanziario. Nello specifico, la Direttiva NIS 2 troverà applicazione per tutti i settori qualificati ad elevata criticità o importanti, mentre la Direttiva CER (anche essa operativa dal 18 ottobre 2024) si applicherà ai c.d. soggetti critici che dovranno essere individuati entro il 17 luglio 2026.

L'Italia ha inoltre adottato la disciplina relativa al c.d. Perimetro di Sicurezza Nazionale Cibernetica che trova la sua prima manifestazione nel D.L. n. 105/2019 e si articola in numerose fonti normative che hanno creato un quadro articolato, la cui finalità dichiarata è quella di garantire un elevato livello di sicurezza dei sistemi informatici dei c.d. settori essenziali, tra cui vi rientrano anche quello bancario e finanziario.

I vari testi legislativi in materia di cybersicurezza hanno istituito nuove Autorità competenti a livello nazionale (*e.g.*, l'Agenzia per la cybersicurezza nazionale) e incaricato di ulteriori poteri di vigilanza e controllo Autorità già esistenti, prevedendo specifici obblighi di cooperazione tra loro.

La proliferazione legislativa a livello nazionale e comunitario in materia di sicurezza informatica comporterà la necessità per gli operatori coinvolti di svolgere una - non sempre agevole - attività di individuazione, mappatura e coordinamento degli obblighi e adempimenti previsti dalle varie fonti normative, nonché la necessità di interfacciarsi con diverse Autorità competenti.

6. COORDINAMENTO TRA IL DORA ED IL REGOLAMENTO (UE) 679/2016 ("GDPR")

Il Regolamento, nonché il *framework* normativo della *cybersecurity*, presenta molti punti di interazione con il GDPR. Questo concretamente comporterà la necessità per le istituzioni finanziare di sviluppare un approccio olistico e integrato nella gestione della sicurezza informatica e dei trattamenti dei dati personali.

In particolare, è possibile individuare i seguenti principali elementi di intersezione tra le due discipline:

1. Gestione delle segnalazioni di incidenti informatici ed eventuali data breach

Il DORA prevede per gli operatori finanziari l'obbligo di notificare gli incidenti informatici alle Autorità competenti e, qualora l'incidente informatico comporti un *data breach* (*e.g.*, accesso non autorizzato, perdita, modifica e/o divulgazione dei dati personali), si dovranno applicare le prescrizioni previste dall'art. 33 del GDPR, che impone l'onere di notificare al Garante Privacy eventuali *data breach* entro 72 ore dalla conoscenza delle stesse, comunicando tutta una serie di informazioni, a titolo esemplificativo la natura della violazione, dei dati personali e dei soggetti interessati coinvolti, nonché le misure di sicurezza (ivi incluse quelle tecnico-informatiche) implementate per minimizzare gli effetti negativi della violazione.

La gestione delle segnalazioni di incidenti informatici, nonché di violazioni di dati personali, comporta per gli operatori finanziari la necessità di individuare - tra le varie fonti normative - gli obblighi di segnalazione, le relative modalità e tempistiche, nonché la necessità di interfacciarsi con le diverse Autorità competenti.

2. Rapporti contrattuali con i fornitori di servizi ICT

Infine, un aspetto centrale riguarda i rapporti contrattuali con i fornitori di servizi ICT, sia sotto il profilo della sicurezza informatica che della protezione dei dati personali.

In particolare, il DORA prevede l'inserimento nei contratti con i fornitori ICT di previsioni disciplinanti gli elementi essenziali del rapporto di esternalizzazione, al fine di garantire un adeguato livello di sicurezza informatica e di controllo, da parte delle istituzioni finanziarie, dei relativi rischi (*e.g.*, individuazione dei livelli di servizio; previsione dei diritti di risoluzione; previsione del diritto di monitorare le prestazione del fornitore dei servizi ICT; i Paesi in cui saranno trattati i dati). Di converso, le istituzioni finanziare dovranno prevedere adeguate garanzie in materia di protezione dati personali, anche ai sensi dell'art. 28 del GDPR (*i.e.*, nomina dei responsabili del trattamento), coordinando tutti gli adempimenti della disciplina del DORA e del GDPR, inclusa la necessità di svolgere eventuali valutazioni d'impatto sulla protezione dei dati personali.

I rapporti commerciali con i fornitori di servizi ICT dovranno essere regolati da contratti che tengano conto di tutti gli adempimenti previsti dalle diverse fonti normative e, per i contratti già in essere, potrebbe essere necessario predisporre specifici *addenda* che, concretamente, potrebbero comportare negoziazioni non sempre agevoli con i fornitori ICT.

7. CONCLUSIONI

Entro la data di entrata in vigore del DORA (17 gennaio 2025), gli operatori finanziari dovranno necessariamente conformarsi alle disposizioni del Regolamento (prevenendo il rischio di irrogazione delle sanzioni amministrative o, eventualmente, penali a cura degli Stati Membri), integrando i nuovi adempimenti con le altre fonti normative rilevanti in materia di *cyber -security* e protezione dati personali.

Al riguardo, occorre segnalare che il DORA costituisce una *lex specialis* rispetto alla futura Direttiva NIS 2 e al contempo prevede per gli enti finanziari la disapplicazione di alcune disposizioni della Direttiva CER. In ogni caso, una delle sfide principali per gli operatori coinvolti consisterà proprio nell'individuare gli obblighi già implementati e quelli da integrare, sulla base delle diverse fonti normative applicabili.

Per le istituzioni finanziarie coinvolte è in conclusione raccomandabile:

- adottare un approccio olistico e integrato nella gestione della sicurezza informatica - considerando anche i rischi per i trattamenti dei dati personali - svolgendo un'attività di individuazione, mappatura e coordinamento degli obblighi previsti dalle varie fonti normative;
- adottare una strategia per la resilienza operativa digitale;
- verificare e coordinare i diversi obblighi di segnalazione degli incidenti informatici e delle violazioni di dati personali;
- implementare adeguati controlli di sicurezza sulla propria infrastruttura digitale, anche attraverso l'individuazione e applicazione di idonee misure tecniche, informatiche e organizzative;
- regolare in via contrattuale il rapporto con i fornitori ICT e, ove necessario, rinegoziare / integrare i contratti già in essere.

CONTATTI

Giancarlo Ranucci
giancarlo.ranucci@lcalex.it

Giulio Vecchi
giulio.vecchi@lcalex.it

Edoardo Raffiotta
edoardo.raffiotta@lcalex.it

Miriam Cugusi
miriam.cugusi@lcalex.it

Davide Machiorlatti
davide.machiorlatti@lcalex.it