DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Tra DORA e GDPR: cybersecurity e privacy nel settore finanziario

16 Maggio 2023

Giangiacomo Olivi, Partner, Dentons
Antonio Venditti, Associate, Dentons

Giangiacomo Olivi, Partner, Europe Co-Head of Intellectual Property, Data and Technology, Dentons

Antonio Venditti, Associate, Dentons

Giangiacomo Olivi

Giangiacomo Olivi è partner presso l'ufficio Dentons di Milano e co-responsabile per l'Europa della practice di Intellectual Property, Data and Technology. Assiste clienti, quali aziende nazionali e internazionali e associazioni industriali, fornendo consulenza legale strategica e commerciale in materia di tecnologia, media e comunicazione, con un focus specifico sulla gestione dei dati e sulla trasformazione digitale.

Studio Legale Tributario

Dentons Europe

大成 DENTONS

In breve

La trasformazione digitale del settore finanziario ha portato molteplici vantaggi ai consumatori, alle imprese e alle autorità di regolamentazione, in termini – ad esempio – di maggiore efficienza, innovazione e concorrenza. Al contempo, però, ha anche esposto il settore finanziario a nuovi peculiari rischi di carattere informatico che, considerata la sempre maggiore dipendenza dei mercati finanziari dalle tecnologie dell'informazione e della comunicazione ("**ICT**"), possono avere un impatto significativo sulla integrità e stabilità finanziaria dell'Unione europea, oltre che sulla protezione dei consumatori europei.

Per affrontare queste sfide, la Commissione europea ha proposto un nuovo quadro legislativo per la resilienza operativa digitale nel settore finanziario – il *Regolamento (UE) 2022/2554 del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario*[1], Digital Operational Resilience Act ("**DORA**") – formalmente adottato il 16 gennaio 2023 e applicabile a decorrere dal 17 gennaio 2025.

Il DORA si applicherà sostanzialmente alla totalità delle società operanti nel settore finanziario (cd. *financial entities* – "**FE**")[2], oltre che ai relativi fornitori di servizi ICT, con l'obiettivo di stabilire un quadro regolamentare comune[3] per:

(i) la corretta ed efficace gestione dei rischi ICT,

1 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

2 Il DORA si applicherà a un'ampia gamma di EF, quali enti creditizi, imprese di investimento, istituti di pagamento, imprese di assicurazione e riassicurazione, società di gestione, fornitori di servizi per le cripto-attività ed emittenti di token collegati a tali attività, nonché società che forniscono servizi ICT a tali entità. Per ulteriori dettagli, l'articolo 2 definisce l'ambito di applicazione del DORA.

3 I principi di cui al DORA saranno implementati attraverso diversi regolamenti delegati della Commissione europea che "daranno vita" ai principi generali e ai requisiti di alto livello stabiliti dal DORA. In effetti, nella stesura del DORA, il legislatore dell'UE sembra aver adottato un approccio simile a quello alla base del Regolamento (UE) 2016/679 del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*, noto anche come ("**GDPR**"). In entrambi i casi, il legislatore dell'UE – piuttosto che definire precise regole di condotta – ha stabilito infatti i principi generali che dovrebbero guidare le FE (o i titolari / responsabili del trattamento) nel garantire, da un lato, la resilienza dei loro sistemi ICT e, dall'altro, la protezione dei dati personali.

vedi l'articolo online

(ii) il monitoraggio dei fornitori di ICT critici,

(iii) la segnalazione e la condivisione di informazioni sugli incidenti ICT, e

(iv) la verifica e l'*auditing* dei sistemi e dei processi ICT.

Il DORA avrà quindi un impatto significativo sulle FE e sui fornitori di servizi ICT nella misura in cui introdurrà – o, quantomeno, rafforzerà – i requisiti e gli standard di sicurezza ICT applicabili al settore finanziario. Ne consegue che le FE (e i fornitori di servizi ICT) avviare quanto prima delle specifiche attività di adeguamento mappando, in primo luogo, gli obblighi che saranno loro imposti dal DORA. Sulla base di tale mappatura, bisognerà poi svolgere una *gap analysis* per comprendere quale sia l'effettivo scostamento rispetto ai requisiti normativi e, alla luce delle risultanze dell'analisi, predisporre un vero e proprio e piano di adeguamento al DORA, il tutto adottando un approccio olistico che prenda in considerazione – non solo il DORA stesso e la relativa normativa secondaria, ma anche – il restante quadro normativo in materia di protezione delle informazioni e dei dati personali[4].

Naturalmente, per quanto qui interessa, il DORA non è destinato a sostituire l'attuale quadro normativo europeo in materia di protezione dei dati personali e, in particolare, il GDPR, ma piuttosto a integrarlo, individuando una serie di adempimenti specifici in materia di sicurezza ICT che – sebbene finalizzati a garantire la resilienza delle FE – saranno anche funzionali a garantire la protezione dei dati personali. Il DORA e il GDPR, infatti, condividono lo stesso obiettivo di garantire la sicurezza, la riservatezza e l'integrità dei dati (personali e non).

In questo articolo riassumiamo le caratteristiche principali del DORA e affrontiamo alcuni dei possibili punti di contatto tra il DORA e il GDPR che potrebbero essere presi in considerazione per ottimizzare le attività necessarie per adeguarsi al DORA.

4 In effetti, la questione è duplice, in quanto, ad esempio, l'articolo 32 del GDPR richiede ai titolari e ai responsabili del trattamento di "*mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

DORA: cinque pilastri per garantire la resilienza ICT della FE

Il DORA può essere suddiviso in cinque "pilastri fondamentali" che, coinvolgendo diversi aspetti della sicurezza informatica, forniscono il quadro di riferimento per la resilienza digitale nel settore finanziario. Le caratteristiche principali di ciascun pilastro possono essere riassunte come segue:

1. ICT Risk Management
    a. Creazione di sistemi e strumenti ICT resilienti che riducano al minimo le conseguenze di eventuali minacce informatiche.
    b. Organizzazione di un sistema di *governance* interna per garantire la corretta gestione dei rischi informatici.
    c. Definizione di una strategia di resilienza digitale in materia di *business continuity* e *disaster recovery*.
2. Segnalazione di incidenti di sicurezza
    a. Implementazione di processi di rilevazione, gestione e registrazione degli incidenti di sicurezza informatica.
    b. Classificazione degli incidenti secondo i criteri che saranno specificati dalle autorità di vigilanza competenti (*e.g.*, a seconda del settore di attività, EBA, EIOPA, *etc.*).
    c. Segnalazione degli incidenti di sicurezza alle autorità competenti (e/o agli utenti delle FE) utilizzando un modello comune e una procedura armonizzata.
3. Resilienza operativa digitale
    a. Test periodici e verifiche per individuare eventuali carenze del sistema di governance ICT adottato.
    b. Adozione di requisiti di resilienza operativa proporzionati alle dimensioni, all'attività e ai pro-

vedi l'articolo online

fili di rischio delle entità[5].

4. Gestione dei rischi informatici derivanti da terzi

   a. Monitoraggio dei rischi derivanti dall'esternalizzazione di servizi ICT a fornitori terzi.

   b. Aggiornamento degli accordi con i fornitori di servizi ICT affinché tali accordi includano alcune disposizioni obbligatoriamente previste dal DORA (*e.g.*, descrizione completa del livello di servizio, l'indicazione dei luoghi in cui i dati vengono trattati, *exit clauses*, audit, *etc.*)

5. Information Sharing

   a. Creazione di un sistema di condivisione su base volontaria delle informazioni su eventuali minacce informatiche rilevate.

L'interazione tra DORA e GDPR: quattro passi per ottimizzare la conformità ICT e privacy delle entità finanziarie

Prendendo in considerazione il GDPR, possono essere individuati diversi punti di contatto con il DORA. Tra questi:

a) Valutazione del rischio ICT e privacy

Secondo il DORA, le FE devono condurre una valutazione completa e regolare del proprio profilo di rischio ICT, che includa l'identificazione, la classificazione e la mitigazione di potenziali cyberattacchi, interruzioni ICT e altre minacce digitali. Dal punto di vista della privacy, tale valutazione deve riguardare anche i rischi di protezione dei dati e, più precisamente, gli scenari aziendali effettivi in cui può verificarsi una violazione dei dati (ad esempio, accesso non autorizzato di un dipendente infedele, perdita di dati causata da misure tecniche insufficienti)[6].

5 Ad esempio, per i livelli più elevati di esposizione al rischio, è necessario condurre un *Threat Led Penetration Testing* (TLTP) completo.

6 A questo proposito, a titolo esemplificativo, la valutazione del profilo di rischio ICT può considerare i risultati delle DPIA condotte dall'azienda, in modo che il processo di raccolta delle informazioni sia più efficace e l'insieme

b) Policy e procedure ICT in materia di sicurezza e resilienza dei sistemi e delle funzioni ICT

Oltre ad adottare policy, procedure e controlli ICT rilevanti per il DORA, le FE devono anche garantire la conformità ai principi e agli obblighi del GDPR (ad esempio, minimizzazione dei dati, limitazione delle finalità, sicurezza dei dati, privacy by design e by default, *etc.*). Un esempio calzante potrebbe essere la prassi di condurre una valutazione di impatto ("**DPIA**"). Infatti, se la soglia di rischio per la conduzione di una DPIA è soddisfatta, è probabile che la FE debba anche rivalutare i livelli di sicurezza dei propri sistemi ICT. Allo stesso modo, la policy relativa alla gestione delle violazioni dei dati dovrebbe occuparsi anche degli obblighi di segnalazione previsti dal DORA (e dal regolamento delegato di prossima adozione). In altre parole, le *policy* e le procedure dovrebbero essere coerenti tra loro e funzionare come "ingranaggi di uno stesso meccanismo", volto a garantire la sicurezza delle ICT e della privacy.

c) Auditing e rapporti con i fornitori ICT

Il DORA dispone che le FE siano tenute a monitorare attivamente i rischi ICT, inclusi quelli derivanti dall'esternalizzazione di servizi e funzioni ICT a terze parti. Per questo fine, dunque, il Capo V del DORA prevede che gli accordi con i fornitori di servizi ICT includano alcune disposizioni "minime", di carattere obbligatorio, per disciplinare gli elementi essenziali di tali rapporti di esternalizzazione[7]. In sostanza, quindi, entro gennaio 2025, le FE dovranno rivedere e aggiornare tutti i rapporti contrattuali con i fornitori di servizi ICT e, in questa attività di adeguamento, è essenziale che le disposizioni e le clausole introdotte come conseguenza del DORA siano coordinate con gli accordi sulla protezione dei dati ai sensi dell'articolo 28 del GDPR. Anche in questa fattispecie

delle misure di sicurezza adottate sia funzionale alla conformità sia al DORA che al GDPR.

7 Secondo l'articolo 30 del DORA, gli accordi stipulati dalle EF per l'utilizzo di servizi ICT esternalizzati devono includere, tra l'altro, quanto segue: "*la descrizione chiara e completa di tutte le funzioni che il fornitore terzo di servizi ICT deve svolgere e tutti i servizi ICT che deve prestare* ", "*le località, segnatamente le regioni o i paesi, in cui si devono svolgere le funzioni e prestare i servizi ICT appaltati o subappaltati e in cui si devono trattare i dati*", "*le disposizioni in materia di disponibilità, autenticità, integrità e riservatezza in relazione alla protezione dei dati, compresi i dati personali* ", "*le descrizioni dei livelli di servizio, compresi relativi aggiornamenti e revisioni*", "*l'obbligo per il fornitore terzo di servizi di ICT di operare senza riserve con le autorità competenti e con le autorità di risoluzione dell'entità finanziaria, comprese le persone da queste nominate*". Si noti che quanto sopra non è esaustivo.

vedi l'articolo online

le FE dovrebbero adottare un approccio olistico per far sì che le diverse disposizioni contrattuali siano correttamente coordinate tra loro. Ad esempio, in tema di audit e verifica dell'affidabilità dei responsabili del trattamento sarà fondamentale adottare una metodologia di verifica unitaria che prenda congiuntamente in considerazione i livelli di sicurezza ICT richiesti ai sensi del DORA e le garanzie richieste al fornitore ICT (*i.e.*, il responsabile *ex* articolo 28 GDPR) in materia di protezione dei dati personali.

d) Formazione in materia cyber e privacy

Sia ai sensi del GDPR che del DORA, le FE sono tenute a fornire istruzioni adeguate ai propri dipendenti e collaboratori in materia di rischi ICT e di obblighi derivanti dalla normativa in materia di protezione dei dati personali. Per quanto qui interessa, un piano di formazione efficace dovrebbe trattare unitariamente di entrambe le tematiche per creare una effettiva consapevolezza aziendale in tema di rischi ICT. A titolo esemplificativo, infatti, le minacce informatiche che possono minare la sicurezza ICT sono sicuramente più ampie (e in parte diverse) rispetto ai rischi privacy strettamente intesi, ma non per questo un piano di formazione efficace dovrebbe concentrarsi solo sugli uni piuttosto che sugli altri.

Conclusioni

Il DORA e il GDPR sono testi giuridici che, seppur tra loro diversi, sono essenziali e complementari per salvaguardare la privacy e garantire la sicurezza informatica del settore finanziario digitale nell'UE. Al contempo, essi pongono sfide e complessità per le FE e i loro fornitori terzi di servizi ICT, che dovranno adottare (e aggiornare, con riferimento al GDPR) piani di adeguamento che tengano conto delle peculiarità di entrambi i quadri giuridici.

Le FE (e i fornitori di servizi ICT soggetti al DORA) dovrebbero quindi prendere in considerazione la possibilità di integrare la gestione del rischio ICT e i principi di protezione dei dati in un unico processo decisionale. Una strategia e un approccio integrati possono facilitare la conformità al GDPR e al DORA, e allo stesso tempo ridurre il livello di esposizione al rischio.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it