CYBERSECURITY NEL SETTORE FINANZIARIO E NON SOLO: IL REGOLAMENTO DORA

DOT FLASH NEWS

CAPPELLI RIOLO
CALDERARO CRISOSTOMO
DEL DIN & PARTNERS

CRCD Studio Legale

INTRODUZIONE

Lo Studio assiste le entità finanziarie nella conformità al Regolamento DORA, supportandole nell'analisi dei rischi TIC, nella gestione dei rapporti con fornitori terzi, nella revisione dei contratti di esternalizzazione e nell'adeguamento delle politiche interne.

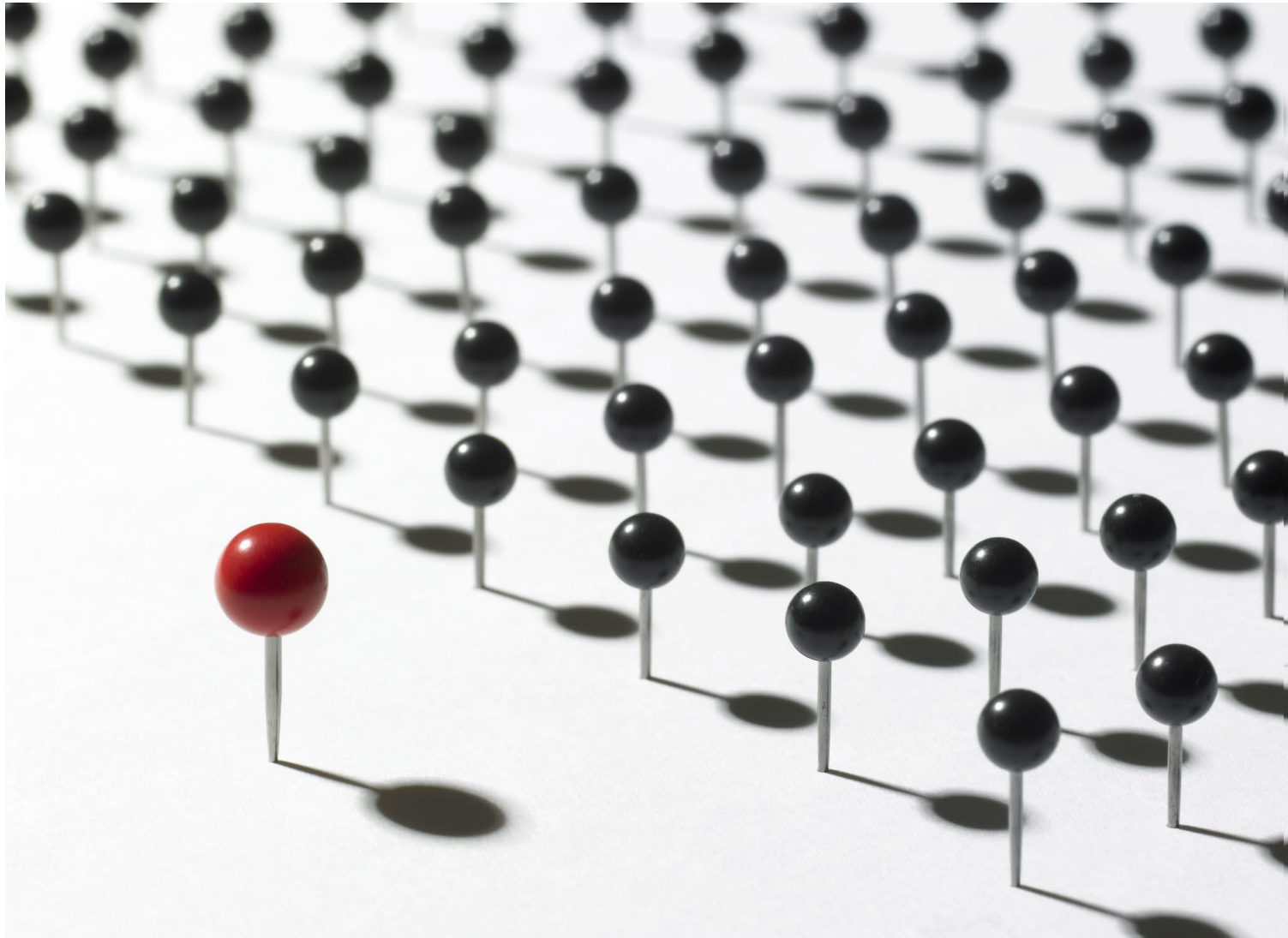
REGOLAMENTO DORA (REG. UE 2022/2254)

Dal **17 gennaio 2025** sono pienamente applicabili le disposizioni del Regolamento DORA (Digital Operational Resilience Act) e delle relative norme tecniche e regolamentari di attuazione (alcune delle quali, tuttavia, devono ancora essere adottate). È attualmente in discussione anche lo schema di decreto legislativo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento DORA.

Il Regolamento stabilisce un quadro normativo uniforme per garantire la **resilienza operativa digitale** del settore finanziario, in risposta alla sempre maggiore dipendenza dalle tecnologie di questo settore e al conseguente aumento del rischio di **attacchi informatici** e **incidenti connessi alle TIC** (Tecnologie dell'Informazione e Comunicazione).

AMBITO DI APPLICAZIONE: NON SOLO ENTITÀ FINANZIARIE

Il Regolamento non riguarda esclusivamente le entità finanziarie: specifiche disposizioni si applicano direttamente anche nei confronti di fornitori terzi critici di servizi TIC, riconoscendo il ruolo centrale di questi ultimi nella catena di fornitura tecnologica.



CRCD Studio Legale

GESTIONE DEL RISCHIO TIC DI TERZE PARTI: FOCUS

- Tra i «pilastri» del Regolamento DORA si segnala in particolare l'insieme di regole volte a gestire il **rischio TIC derivante da terze parti**, ossia dai fornitori terzi a cui le entità finanziarie esternalizzano i servizi TIC, *i.e. «servizi digitali e di dati forniti attraverso sistemi di TIC ad uno o più utenti interni o esterni su base continuativa, inclusi l'hardware come servizio e i servizi hardware, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di software e firmware da parte del fornitore dell'hardware, esclusi i servizi telefonici analogici tradizionali».*
- Alcuni esempi di servizi TIC: concessione di **licenze software**, **servizi cloud** (IaaS, PaaS, SaaS), **fornitura di infrastrutture di rete**, **Hardware as a Service** e **servizi di assistenza tecnica**, comprese le attività di aggiornamento software e firmware fornite dal produttore dell'hardware.
- Per mitigare il rischio derivante dall'esternalizzazione, le entità finanziarie devono adottare misure organizzative e contrattuali specifiche con i fornitori terzi di servizi TIC.

CONTRATTI PER L'UTILIZZO DI SERVIZI TIC

Prima della conclusione di qualsiasi contratto con fornitori terzi di servizi TIC è obbligatorio svolgere una specifica **analisi precontrattuale**, che include un'attività di ***due diligence*** sulle **qualifiche e caratteristiche del fornitore**.

I contratti con i fornitori terzi di servizi TIC devono rispettare i requisiti minimi definiti dal Regolamento DORA, distinguendo a seconda che il servizio TIC sia utilizzato o meno a supporto di **funzioni essenziali o importanti**.

Questi elementi includono previsioni che impattano anche sul **trattamento dei dati personali** da parte dei fornitori.

COME PROCEDERE?

- I **contratti di esternalizzazione già in essere**, aventi ad oggetto servizi TIC, devono essere **rinegoziati** dall'entità finanziaria per renderli conformi al Regolamento DORA.
- I **nuovi contratti di esternalizzazione** devono essere redatti e negoziati tenendo conto dei **nuovi requisiti normativi**.

In entrambi i casi, è consigliabile che l'entità finanziaria si doti di un proprio **modello contrattuale standard**, da sottoporre a ciascun fornitore con le personalizzazioni del caso, per assicurare la conformità al Regolamento DORA.

Flash news a cura del team IP-IT & Privacy:
Alessandra Feller – alessandra.feller@crccdlex.com
Giulia Iozzia – giulia.iozzia@crccdlex.com
Ginevra Lombardi – ginevra.lombardi@crccdlex.com