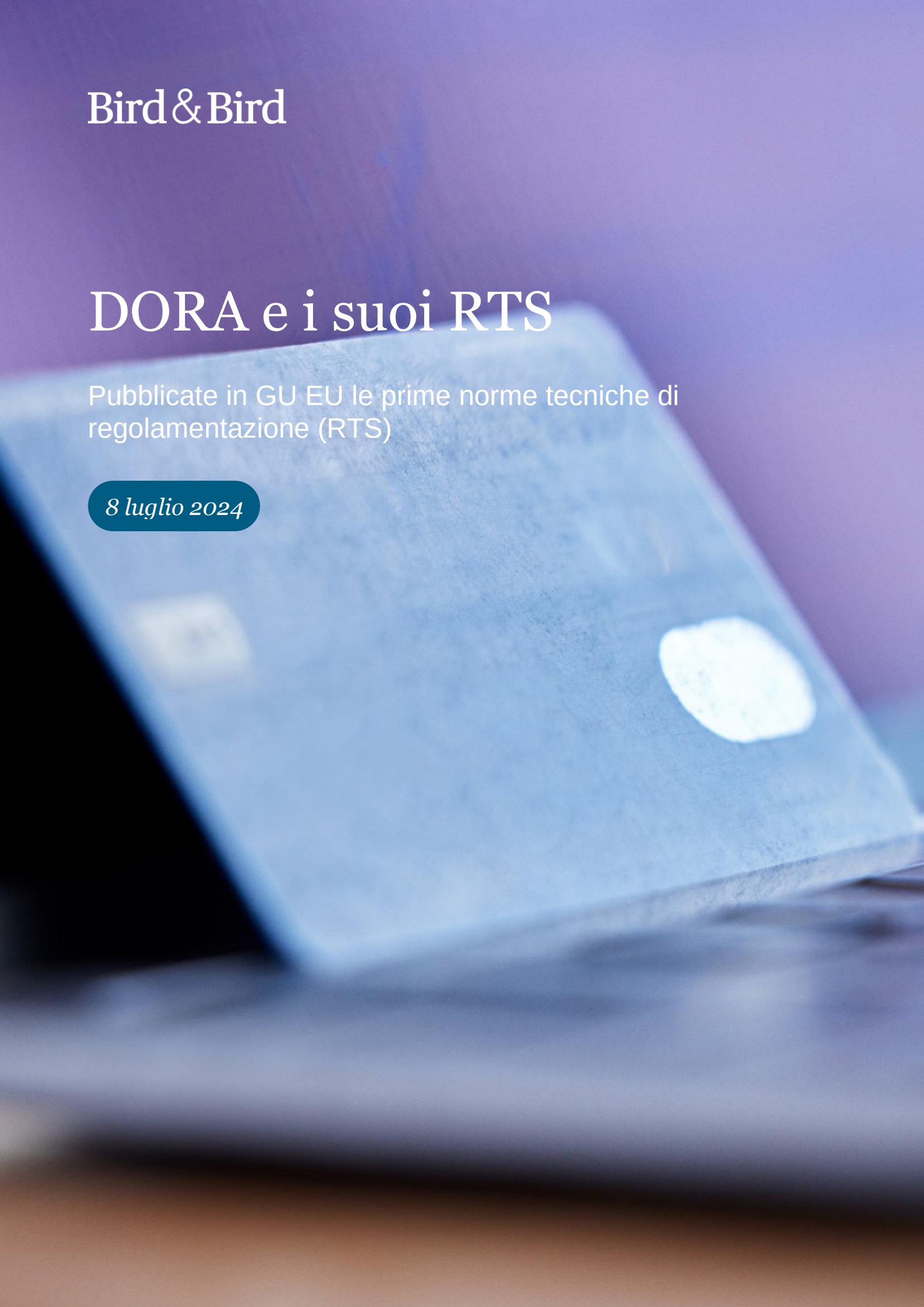
Bird & Bird

DORA e i suoi RTS

Pubblicate in GU EU le prime norme tecniche di regolamentazione (RTS)

8 luglio 2024



Regolamento DORA: pubblicate in GU EU le prime norme tecniche di regolamentazione

Come noto, il 17 gennaio 2025 entrerà in applicazione il **Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio sulla resilienza operativa digitale per il settore finanziario (DORA)**.

DORA mira ad armonizzare le regole di ICT Governance e ICT Risk Management per le entità finanziarie nell'UE, applicando un principio di proporzionalità basato sul rischio. Questo approccio garantisce una gestione omogenea e coerente dei rischi ICT nei vari segmenti del settore finanziario.

Per raggiungere questi obiettivi, DORA stabilisce una disciplina univoca per la segnalazione degli incidenti, i test di resilienza operativa e la gestione dei rapporti tra entità finanziarie e fornitori terzi di servizi ICT. Inoltre, introduce un quadro di vigilanza paneuropeo per i fornitori terzi di servizi ICT considerati critici.

Le entità finanziarie soggette a DORA devono definire e implementare una strategia di resilienza operativa digitale allineata alla loro strategia aziendale. Questo processo rappresenta il risultato di una convergenza verso uno *standard* regolamentare che valorizza le linee-guida emesse dalle Autorità europee di supervisione (ESA) in materia di *governance* della tecnologia digitale, rischi ICT e rapporti con prestatori terzi di servizi ICT. Basato sull'analisi del quadro normativo pregresso e sull'esperienza applicativa, DORA richiede alle entità finanziarie di integrare la *governance* del rischio ICT, comprendente ruoli e responsabilità, politiche, processi, strumenti e meccanismi di comunicazione e coordinamento organizzativo, nella loro Corporate Governance.

Per un'applicazione organica della normativa, DORA prevede la **specificazione di requisiti già presenti attraverso norme tecniche di regolamentazione e norme tecniche di implementazione** elaborate dalle Autorità di vigilanza europee (European Banking Authority, European Securities and Markets Authority ed European Insurance and Occupational Pensions Authority; c.d. ESA), e rese cogenti dalla Commissione Europea attraverso regolamenti delegati.

In tale contesto, lo scorso 25 giugno sono stati pubblicati in Gazzetta Ufficiale dell'Unione Europea i primi regolamenti delegati previsti da DORA:

- il **Regolamento delegato (UE) 2024/1772** del 13 marzo 2024 che integra il Regolamento DORA per quanto riguarda gli *standard* tecnici relativi ai **criteri per la classificazione degli incidenti connessi alle ICT** e delle minacce informatiche, alle soglie di rilevanza ed ai dettagli delle segnalazioni di gravi incidenti;
- il **Regolamento delegato (UE) 2024/1773** del 13 marzo 2024 che integra il Regolamento DORA con gli *standard* tecnici di attuazione relativi al contenuto dettagliato della **politica relativa agli accordi contrattuali per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti prestati da fornitori-terzi**;
- il **Regolamento delegato (UE) 2024/1774** del 13 marzo 2024 che integra il Regolamento DORA per quanto riguarda le norme tecniche di regolamentazione che specificano gli strumenti, i metodi, i processi e le politiche per la **gestione dei rischi informatici** e il quadro semplificato per la gestione dei rischi informatici.

Tali provvedimenti, inclusi nel primo *batch* di norme tecniche poste in consultazione dalle ESAs dal 19 giugno all'11 settembre 2023, fanno parte del più ampio set di norme attuative del Regolamento (UE) 2022/2554, il cui obiettivo è quello di sviluppare un **approccio pienamente armonizzato alla finanza digitale per facilitare l'adozione sicura della tecnologia** da parte delle istituzioni finanziarie.

Regolamento delegato (UE) 2024/1772

Il Regolamento delegato 2024/1772 specifica i criteri per la classificazione degli incidenti informatici e le soglie di rilevanza per la determinazione dei gravi incidenti e delle minacce informatiche significative, ai sensi di quanto stabilito dall'art. 18 del DORA.

I criteri di classificazione e le soglie di rilevanza ivi previsti riflettono le dimensioni e il profilo di rischio complessivo dell'ente finanziario, nonché la natura, la portata e la complessità dei servizi di tutte le entità finanziarie: sono quindi concepiti in modo tale da essere applicati in modo coerente a tutte le entità finanziarie, indipendentemente dalle loro dimensioni e dal loro profilo di rischio, e non comportare un onere di segnalazione sproporzionato per le entità finanziarie più piccole.

In relazione alle previsioni in tema di segnalazione degli incidenti, che esistevano prima dell'entrata in vigore del DORA, è stata garantita la continuità per le entità finanziarie, e, pertanto, i criteri di classificazione e le soglie di rilevanza recati dal Regolamento delegato 2024/1772 sono da intendersi allineati:

- agli Orientamenti EBA sulla segnalazione degli incidenti gravi ai sensi della Direttiva (UE) 2015/2366;
- agli Orientamenti sulle informazioni periodiche e sulla comunicazione delle modifiche sostanziali che i repertori di dati sulle negoziazioni devono presentare all'ESMA;
- al quadro di riferimento della BCE/SSM per la segnalazione degli incidenti informatici e ad altri orientamenti pertinenti.

Nello specifico, i criteri di classificazione degli incidenti ICT riguardano:

- i clienti, le controparti e le transazioni impattate;
- la perdita dei dati;
- l'impatto reputazionale;
- la durata e il periodo di inattività;
- l'estensione geografica;
- l'impatto economico;
- la criticità dei servizi colpiti.

Per ciascun criterio sono poi specificate le relative soglie di rilevanza che, se raggiunte, permettono la classificazione dell'incidente ICT come grave. Tali soglie si basano sul numero dei clienti, delle controparti e delle transazioni interessati, sulla durata dell'incidente e dell'inattività del servizio, sul numero di Stati coinvolti, sulla qualità dei dati e sull'ammontare di costi e perdite.

Le minacce informatiche significative vengono classificate in base alla probabilità di materializzazione della minaccia, all'eventuale incidenza della stessa su funzioni critiche o importanti delle entità finanziarie, e al fatto che la minaccia informatica potrebbe soddisfare le condizioni per essere classificata come incidente ICT grave se si dovesse materializzare.

La classificazione degli incidenti ICT in base alla loro criticità e all'importanza dei servizi coinvolti mira a garantire una registrazione accurata per il monitoraggio, la gestione e la risoluzione degli stessi, in conformità con il processo organizzativo interno di gestione degli incidenti ICT che ogni entità finanziaria deve definire e implementare. Inoltre, tale classificazione è essenziale per adempiere all'obbligo di segnalare gli incidenti gravi all'autorità nazionale competente.

Regolamento delegato (UE) 2024/1773

Il Regolamento delegato (UE) 2024/1773 delinea i principi che le entità finanziarie devono riflettere nelle proprie politiche relative agli accordi contrattuali con fornitori-terzi per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti, che le medesime entità finanziarie devono adottare – e riesaminare periodicamente – ai sensi dell'art. 28 del DORA.

Tra i principi enucleati dal Regolamento delegato (UE) 2024/1773, merita in particolare segnalare che:

- le entità finanziarie devono trattare il rischio ICT di terzi all'interno del loro quadro di gestione del rischio ICT;
- è attribuita all'organo di gestione la responsabilità finale nell'affrontare i rischi informatici di un'entità finanziaria: ciò implica il costante coinvolgimento di tale organo nel controllo e nel monitoraggio della gestione dei rischi informatici, anche attraverso l'adozione e il riesame, almeno una volta all'anno, della *policy* di rischio per l'uso di servizi ICT prestati da fornitori terzi;
- la *policy* deve specificare regole, responsabilità e processi del ciclo di vita dell'accordo contrattuale con un fornitore terzo di servizi ICT, tra cui:
  - meccanismi di *governance*: responsabilità interne per l'approvazione, la gestione e il controllo degli accordi contrattuali pertinenti;
  - responsabilità dell'organo di gestione, compreso l'eventuale coinvolgimento nel processo decisionale sull'utilizzo di servizi ICT resi da fornitori terzi;
  - pianificazione degli accordi contrattuali, tra cui la valutazione dei rischi *ex-ante*, la *due-diligence* e il processo di approvazione di nuovi accordi o di modifiche sostanziali di tali accordi;
  - coinvolgimento delle unità aziendali e delle funzioni di controllo interno nelle diverse fasi di gestione;
  - modalità di attuazione, monitoraggio e gestione degli accordi contrattuali;
  - documentazione e tenuta dei registri (tra cui il registro di informazioni relativo a tutti gli accordi contrattuali con fornitori terzi di servizi ICT);
- elementi strutturali delle strategie di uscita e processi di risoluzione degli accordi contrattuali;
- la *policy* deve inoltre definire un processo adeguato e proporzionato da attuarsi *ex ante* per selezionare i potenziali fornitori terzi di servizi ICT e valutarne l'idoneità (c.d. *due diligence*) e prescrivere che l'entità finanziaria prenda in considerazione un elenco non esaustivo di elementi di valutazione relativi ai fornitori terzi di servizi ICT oggetto di scrutinio.

Regolamento delegato (UE) 2024/1774

Il Regolamento delegato (UE) 2024/1774 specifica, rispettivamente, gli strumenti, i metodi, i processi e le politiche di gestione del rischio ICT per le entità finanziarie e il quadro semplificato di gestione del rischio ICT per le sole entità finanziarie previste dall'art. 16 del DORA.

Le entità finanziarie dovranno, in particolare, ai sensi del DORA e del menzionato Regolamento delegato:

- adottare politiche di sicurezza ICT (tra cui controlli crittografici) per preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati;
- stabilire la metodologia e la procedura per condurre la valutazione del rischio ICT;
- monitorare le vulnerabilità e le minacce interne ed esterne ai sistemi e alle operazioni ICT;
- adottare una politica (e relative procedure) per la gestione degli *asset* ICT (compreso i dati);
- attuare una rigorosa separazione degli ambienti di produzione delle risorse ICT dagli ambienti in cui i sistemi di ICT sono sviluppati e testati o da altri ambienti non di produzione, che funga da importante misura di sicurezza contro l'accesso non intenzionale e non autorizzato, e contro le modifiche e le cancellazioni dei dati nell'ambiente di produzione;
- garantire una comunicazione tempestiva e trasparente delle potenziali minacce alla sicurezza che potrebbero avere un impatto sull'entità finanziaria e sui suoi portatori di interessi;
- garantire che i pacchetti *software* che le entità finanziarie acquisiscono e sviluppano siano integrati in modo efficace e sicuro nell'ambiente ICT esistente, conformemente agli obiettivi aziendali e di sicurezza delle informazioni stabiliti;
- disporre di solide politiche e procedure di gestione delle modifiche delle risorse ICT;
- definire una politica relativa agli incidenti connessi alle risorse ICT che comprenda un processo di gestione degli incidenti;
- raccogliere, monitorare e analizzare le diverse fonti di informazione e assegnare i relativi ruoli e responsabilità, non limitandosi a fare affidamento solo sui *log*;
- conservare le prove degli incidenti connessi alle risorse ICT, determinandone il periodo di conservazione, e tenendo conto, tra l'altro, della criticità dei dati e degli obblighi di conservazione derivanti dal diritto dell'Unione;
- adottare ed implementare una politica di sicurezza fisica e ambientale (relativa a locali, centri dati, aree sensibili designate e apparecchiature *hardware*).

Next steps

Le norme recate dai Regolamenti Delegati entreranno in vigore il 17 luglio, 20 giorni dopo la pubblicazione ufficiale sulla Gazzetta dell'UE.

Nelle prossime settimane si attende l'approvazione del secondo *batch* di norme tecniche di secondo livello. Nel dettaglio:

- RTS e ITS sul contenuto, tempistica e modalità di notifica dei incidenti ICT significativi;
- Linee-guida su stima dei costi/perdite aggregati derivanti da incidenti ICT gravi;
- RTS sugli accordi di subfornitura di servizi ICT che supportano una funzione critica o importante;
- RTS sulla condotta di vigilanza dei fornitori-terzi di servizi ICT critici;
- Linee-guida sulla cooperazione in materia di vigilanza tra le ESA e le autorità competenti;
- RTS sui test di penetrazione guidati dalle minacce (TLPT).

In termini generali merita, infine, rammentare che **dal 17 gennaio 2025 il DORA sarà direttamente applicabile in tutti gli Stati membri dell'UE**.

Ciò significa che sia le entità finanziarie che i fornitori di servizi ICT dovranno **rapidamente apportare le misure necessarie (incluse le modifiche di carattere organizzativo) per assicurare la piena conformità al DORA**.

In particolare, l'applicazione di DORA comporterà la pianificazione ed esecuzione di interventi per adeguare le politiche, i processi, le procedure e gli strumenti di gestione della sicurezza (e dell'affidabilità) dei sistemi ICT, nonché il contenuto e la gestione degli accordi contrattuali, sia tra gli enti finanziari e i fornitori di servizi ICT, sia tra i fornitori di servizi ICT e i loro subappaltatori (ove consentito dall'ente finanziario).

Per quanto riguarda gli accordi con terze parti, vale peraltro la pena notare che, a differenza di quanto disposto dagli Orientamenti EBA in materia di *outsourcing*, **i requisiti contrattuali stabiliti dal DORA si applicano sostanzialmente a qualsiasi accordo per la fornitura di servizi ICT, che si tratti o meno di *outsourcing***.

Si tratta, pertanto, di un'attività particolarmente impegnativa.

Consigliamo a tutte le entità finanziarie e ai fornitori di servizi ICT di **verificare attentamente il proprio stato di adeguamento alle previsioni di DORA** al fine di assicurare la conformità entro i termini previsti.

Per qualsiasi esigenza di chiarimento o di assistenza in merito a quanto precede, i nostri professionisti sono a Vostra completa disposizione.

Contatti

Stefano Febbi

Partner

+390230356000
stefano.febbi@twobirds.com

Giuseppe D'Agostino

Of Counsel

+390230356000
giuseppe.dagostino@twobirds.com

Gian Marco Rinaldi

Counsel

+390230356000
gianmarco.rinaldi@twobirds.com

Diego Cefaro

Senior Associate

+390669667000
diego.cefaro@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Shenzhen • Singapore • Stockholm • Sydney • Warsaw