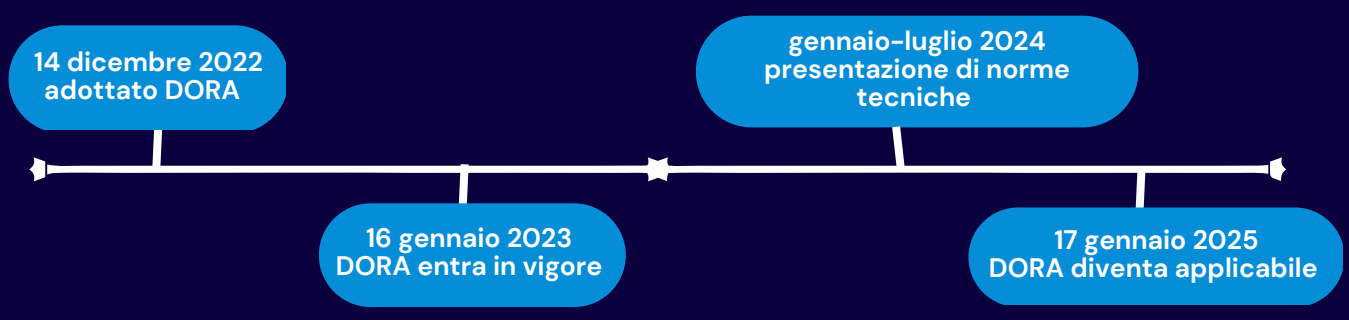
Il Regolamento DORA

Il 14 dicembre 2022 è stato adottato il **Regolamento DORA** ("Digital Operational Resilience Act") che ha l'obiettivo di consolidare e armonizzare a livello europeo la **resilienza operativa digitale** nel settore finanziario

Resilienza operativa digitale: capacità delle imprese di poter resistere ad ogni tipo di perturbazione e minaccia connessa a ICT



A chi si applica DORA?

DORA si applica a

- **enti finanziari di stampo "tradizionale":** banche, imprese di investimento, assicurazioni
- **nuovi attori del mercato** (es. aziende di servizi di cripto-*asset*) e **fornitori critici di servizi ICT** (es. fornitori di servizi cloud)

Mentre DORA

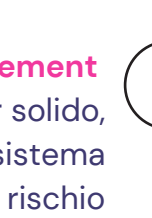
- si applica in forma semplificata ad alcuni enti (es. micro imprese)
- non si applica ad alcuni soggetti (es. imprese di assicurazione e riassicurazione sotto determinate soglie di dimensioni)

I quattro pilastri di DORA

Le entità finanziarie dovranno

1 **Governance e organizzazione interna**

Dotarsi di un sistema interno di governance cybersecurity e un quadro di controllo per garantire una gestione efficace e prudente di tutti i rischi ICT



Risk management 2

Disporre di un quadro di gestione del rischio cyber solido, completo e ben documentato come parte del sistema complessivo di gestione del rischio

3 **Incident management e reporting**

- Implementare politiche di continuità operativa, sistemi e piani di ripristino in caso di disastro relativo alle ICT, quale conseguenza di un cyberattacco
- Dotarsi di capacità e personale idonei a rilevare vulnerabilità, minacce, incidenti e attacchi informatici

Fornitori terzi di servizi ICT 4

Introdurre meccanismi di monitoraggio e tutela (anche via contrattuale) dai rischi derivanti da fornitori terzi di servizi ICT

Come prepararsi?

Gap analysis

Revisionare la struttura di governance interna e le misure di gestione dei rischi e incidenti ICT già adottate

Valutare le capacità dell'azienda in ambito di reportistica e implementare o adeguare le esistenti procedure di segnalazione degli incidenti

Incident reporting

Valutazione dei fornitori ICT

Mappare i contratti con i fornitori terzi di ICT, valutandone la criticità, revisionando e documentando le vulnerabilità per pianificare un'adeguata strategia di contenimento del rischio e rinegoziare gli obblighi delle parti

Vuoi saperne di più? Contattata i professionisti di DLA Piper e seguici su Diritto al Digitale