CYBERSECURITY IN THE FINANCIAL SECTOR AND BEYOND: THE DORA REGULATION

DOT FLASH NEWS

CAPPELLI RIOLO
CALDERARO CRISOSTOMO
DEL DIN & PARTNERS

Studio Legale

INTRODUCTION

The Firm assists financial entities in complying with the DORA Regulation, supporting them in analysing ICT risks, managing relationships with third-party suppliers, reviewing outsourcing contracts and adjusting their internal policies.

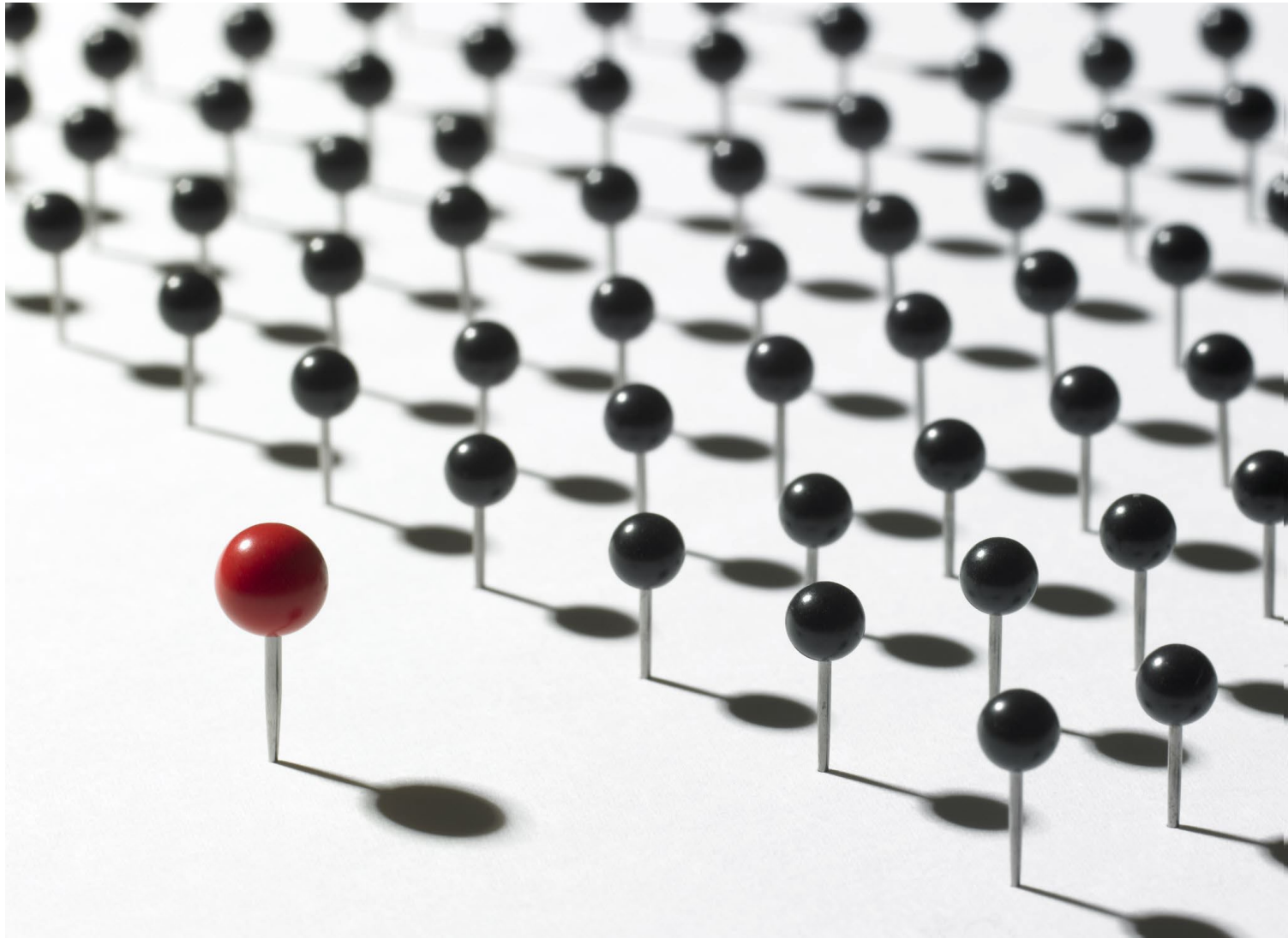
DORA REGULATION (EU REG. 2022/2254)

As of **17 January 2025**, the provisions of the **DORA Regulation (Digital Operational Resilience Act)** and its related implementing and regulatory technical standards are fully applicable (although some of these standards have not been adopted yet). Additionally, the Italian draft legislative decree is currently under discussion to align national laws with the provisions of DORA.

The Regulation establishes a uniform regulatory framework to ensure the **digital operational resilience** of the financial sector, addressing the increasing reliance on technology in this industry and the associated rise of **cybersecurity threats** and ICT (Information and Communication Technology) **incidents**.

SCOPE: NOT JUST FINANCIAL ENTITIES

The Regulation does not apply exclusively to financial entities. Specific provisions also directly affect critical third-party ICT service providers, recognizing their central role in the technological supply chain.



Studio Legale

THIRD-PARTY ICT RISK MANAGEMENT: KEY FOCUS

- One of the «pillars» of the DORA Regulation is the set of rules aimed at managing **ICT risk arising from third parties**, i.e. external providers to whom financial entities outsource ICT services. These services include "*digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including Hardware as a Service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*".
- Examples of ICT services include **software licensing**, **cloud services** (IaaS, PaaS, SaaS), **network infrastructure provision**, **Hardware as a Service**, and **technical support services**, including software and firmware updates provided by the hardware manufacturer.
- To mitigate risks associated with outsourcing, financial entities must adopt specific organizational and contractual measures with third-party ICT service providers.

CONTRACTS FOR ICT SERVICES

- Prior to the conclusion of any contract with ICT third-party service providers, a mandatory **pre-contractual analysis** must be carried out, including a specific **due diligence** on the provider's **qualifications** and **capabilities**.

- Contracts with ICT third-party service providers must comply with the minimum requirements set by the DORA Regulation, distinguishing between **services supporting** critical or important functions and services not supporting such functions.

  These requirements also impact on how providers handle **personal data**.

HOW TO PROCEED?

- **Existing outsourcing contracts** to ICT services must be **renegotiated** by financial entities to ensure compliance with the DORA Regulation.
- **New outsourcing contracts** must be drafted and negotiated in accordance with the **new legislative requirements**.

In both cases, it is advisable for financial entities to develop a **standardized contractual model**, which can be customized as needed for each provider, ensuring compliance with the DORA Regulation.

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