EU Digital Operational Resilience Act (DORA)
A Guide for Technology Providers

Arnon, Tadmor-Levy
Emerging Technologies Practice

Roy Keidar | Ran Yosef

ARNON
ARNON, TADMOR-LEVY

Introduction and Background

This Guide is designed to provide a comprehensive overview on the European Digital Operational Resilience Act's (DORA) which is in effect starting from January 17, 2025.

DORA is part of a broader effort of the EU to establish a robust cybersecurity framework. This effort includes the enactment of the NIS 2 Directive (addressing cyber-security resilience in critical sectors), and the recently approved Cyber Resilience Act (imposing cyber-security requirements for manufacturers and retailers of software or hardware products).

DORA itself aims to protect the continued operation of EU's financial sector. It does so by imposing obligations on EU financial entities regarding their information and communication technology ("ICT") systems. DORA is accompanied by a series of implementing and delegated acts specifying how its obligations are to be interpreted and enforced.

Who does DORA apply to?

DORA generally applies to two groups of entities:

1. European financial entities.
2. Providers of ICT services to such institutes, **whether they are established in the EU or in third countries.**

Therefore, Israeli companies, working in the EU or providing services or products to EU financial entities, would have to be compliant with DORA's requirements.

Financial Entities Under DORA

DORA applies, first and foremost, to financial entities, among which are credit institutions, investment firms, payment institutions, insurance companies, credit rating agencies, and crypto-asset service providers. Covered financial entities are required to comply with DORA's obligations or risk monetary penalties and even permanent cessation of certain conducts.

DORA requires **covered financial entities** to comply with 5 types of obligations (commonly referred to as DORA's 5 pillars):

1. **ICT Risk Management** - establish a robust framework to handle ICT risks, including setting up policies, tools, and procedures to identify, detect and manage ICT risks while monitoring providers of ICT systems.
2. **ICT incident management** - maintain a uniform process to detect, classify, record and report ICT incidents and cyber-security threats.
3. **Digital Operational Resilience Testing** - implement a rigorous testing program for ICT systems, with which ICT third-party service providers would be required to cooperate.
4. **Third-party ICT Risk Management** - address risks emanating from their use of ICT services provided by third parties. This includes the adoption of a third-party ICT risk strategy, upholding minimal contractual components governing the relationship with the ICT third-party service providers, and ensuring they uphold appropriate operation standards.
5. **Information Sharing and Cyber Testing** - financial entities may exchange information to enhance operational resilience and join regulator-led cross-sector crisis management plans.

ICT Third-Party Service Providers Under DORA #1: DEFINITIONS

DORA defines “ICT third-party service providers” as “an undertaking providing ICT services”.

“ICT services” are broadly defined as:

- Digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis.
- Includes hardware as a service and provision of technical support via software or firmware updates by the hardware provider.
- Excludes traditional analogue telephone service.

In practice, key services deemed ICT services include SaaS, ICT security management services, data analytics, payment processing and payment infrastructure, electronic communication services, and more.[1]

[1] For a more comprehensive list, see Annex III to DORA’s Regulatory Technical Standards on register of information, 2.12.2024.

ICT Third-Party Service Providers Under DORA #2: DESIGNATION

To determine what obligations apply to ICT third-party service providers, it is first important to note that DORA has in fact 3 designations of such providers. Our table below details the differences between these designations:

	ICT Third-party Service Provider	ICT Third-party Service Provider supporting critical or important functions	Critical ICT Third-party Service Provider
Definition under DORA	Undertaking providing ICT services.	Supporting a function whose disruption risks financial harm, service continuity, or regulatory compliance for a financial entity.	An ICT third-party service provider designated as critical in accordance with Art. 31
Entity empowered to designate	Financial entities	Financial entities	A regulatory authority appointed per DORA (Lead Overseer)
Criteria for designation	Unspecified	Unspecified	• impact on financial services • importance of the financial entities • reliance for critical or important functions • degree of substitutability of the service provider
How DORA applies	Indirectly, through contractual obligations	Indirectly, through contractual obligations	Directly governed by DORA through a Lead Overseer

ICT Third-Party Service Providers Under DORA #3: OBLIGATIONS

The obligations imposed by DORA, whether directly or indirectly, vary depending on the designation of the ICT Third-Party Service Provider:

1. **ICT Third-Party Service Providers:**

- **Risk Mitigation:** Cooperate with the financial entity's risk controls associated with ICT services.
- **Due Diligence:** Support the financial entity's pre-engagement due diligence.
- **Security Standards:** Comply with relevant information security standards
- **Contractual Obligations:** Fulfill specific contractual requirements, including:
  - Protecting data, including personal data.
  - Ensuring data access in cases of insolvency or contract termination.
  - Support during ICT incidents.
  - Collaboration with regulatory authorities.
  - Participating in training and ICT security awareness programs.

2. **Providers Supporting Critical or Important Functions:** The above obligations apply for Providers supporting critical or important functions, with additional obligations:

- **Notifications:** Report on developments affecting service delivery.
- **Contingency Planning:** Implement and test business continuity plans.
- **Operational Testing:** Participate in the financial entity's digital operational tests.
- **Audits:** Cooperate with inspections and audits by the financial entity.
- **Transition Support:** Assist during the contractual transition period.

3. **Critical ICT Third-Party Service Providers:** Providers designated as "critical" by a Lead Overseer, face additional requirements and are directly subject to DORA:

- **Regulatory Cooperation:** Respond to requests and cooperate with investigations or inspections (including on-site) by lead overseer.
- **Local Presence:** Establish a European subsidiary within 12 months of being designated as a critical provider.
- **Penalties:** Non-compliance may lead to daily fines up to 1% of the average global turnover.

What can we do for you?

We are aware that navigating through DORA regulations can be complex. Our emerging technologies team is equipped with providing our clients practical and comprehensive consultation, including negotiating contractual provisions governing ICT services with EU financial entities, mapping gaps in existing technological infrastructure, and assisting in the preparation for DD processes.

Our team:

Roy Keidar
Leading Partner, Emerging Technologies and AI,
Fintech, Blockchain and Crypto
royk@arnontl.com

Ran Yosef
Emerging Technologies and AI, Fintech,
Blockchain and Crypto
ran.y@arnontl.com

This publication is provided as a service to our clients and colleagues, with explicit clarification that each case requires individual examination. The information presented is for general informational purposes only and is not a substitute for professional advice. While we strive for accuracy, we cannot guarantee the information is up to date on the day it is received or accurate in the future. Do not act based on this without comprehensive professional advice tailored to your unique circumstances.