HERZOG
HERZOG FOX & NEEMAN

Prepare for EU's new Regulation on Cybersecurity and Operational Resilience in the Financial Sector

(**D**igital **O**perational **R**esilience **A**ct)

January 2023

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

Introduction

The EU has enacted the new Regulation on Digital Operational Resilience for the Financial Sector (**"Digital Operational Resilience Act"** or **"DORA"**).

The new regulation will start to **apply from 17 January 2025. Although the application date of DORA may seem as distant, the 24-months period given to covered businesses to comply is relatively tight, considering the significant amount of new regulatory requirements.**

To assist covered businesses to already start getting acquainted with DORA's provisions and take actions to adequately prepare for compliance with its new obligations, we are pleased to present this guidance. The guidance provides a general overview of **DORA's key regulatory requirements** and the **practical next steps** that should be taken.

The Digital Operational Resilience Act

DORA is part of the EU's **Digital Finance Package,** alongside the comprehensive Regulation on Markets in Crypto Assets (MICA). It creates a harmonized detailed and comprehensive **regulatory framework for cybersecurity and operational resilience in the financial sector.**

DORA presents a **wide array of regulatory requirements** aimed at strengthening the security of network and information systems involved in business processes of **financial entities**, in response to the growing threat of cyber-attacks which can cause severe operational disruptions to the financial sector.

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

Who DORA Applies to?

DORA applies to a wide array of entities operating in the financial sector:

Financial Entities

- investment firms
- payment institutions
- electronic money institutions
- crypto-asset services providers,
- issuers of crypto-assets or of certain stablecoins
- credit institutions
- managers of alternative investment funds
- data reporting service providers
- account information services providers
- central securities depositories
- central counterparties
- trading venues
- trade repositories
- management companies
- insurance and reinsurance undertakings
- insurance intermediaries
- reinsurance intermediaries and ancillary insurance intermediaries
- institutions for occupational retirement provision
- credit rating agencies
- administrators of critical benchmarks
- crowd funding service providers
- securitization repositories

Third-party providers of information and communication technologies ("ICT") services

- widely defined as providers of *"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"*, and including:
  - cloud computing services
  - software
  - data analytics services
  - providers of data centre services

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

Key Regulatory Requirements

ICT risk management

Financial Entities will be required to establish a **proper governance and control framework for assessment and management of risks related to ICT**. This framework shall include a wide array of **policies, procedures, protocols, tools and communication strategies**, focusing on **ICT business continuity, resilience** as well as **recovery and restoration methods** to ensure **high standards of availability, authenticity, integrity and confidentiality of data.** Such framework should also address the risks associated with the **use of third-party providers of ICT services** as an integral component of the risk assessment and risk mitigation procedures and mechanisms, taking into account the nature, scale, complexity and criticality of the ICT-related dependencies as well as the risks arising from the contractual arrangements on the use of the ICT services. We note that **simplified regulatory requirements** will apply to **some Financial Entities**, such as small and non-interconnected investment firms, certain exempt payment institutions and electronic money institutions.

Incident management and reporting requirements

Financial Entities will be required to define, establish and implement **process for ICT-related incident management,** with an aim of **detection, management and notification** of such incidents. DORA will require Financial Entities to **record all such incidents** and **significant cyber threats**, as well as to establish proper **procedures and processes for ensuring appropriate monitoring, handling and follow-up** of such incidents. Furthermore, DORA will simplify and utilize the **process for reporting incidents** related to ICT, by consolidating the current multiple reporting channels and standardizing templates. With this context, DORA will require Financial Entities to **report "major" ICT-related incidents to the competent authorities** within tight time limits in the regulation using standard templates, and in some instances also to **inform their clients** about such incident and the mitigation measures taken in that regard.

Digital operational resilience testing

Financial Entities will be required to establish, maintain and review sound and comprehensive **digital operational resilience testing program**, which will include the range of assessments, testing methodologies, practices and tools that will be applied. Under DORA, the tests need to be conducted by **independent parties**, whether internal or external. Furthermore, DORA will require **certain Financial Entities** to carry out advanced testing of ICT tools, systems and processes by means of **threat-led penetration testing (TLPT) at least once in three years.**

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

Cooperation and information sharing arrangements

DORA encourages the sharing of **cyber threat information** among trusted Financial Entities, in order to increase awareness of new cyber threats. This information sharing will need to be implemented by **information-sharing arrangements**, and shall be reported to the relevant competent authority.

Contractual arrangements with ICT third-party service providers

DORA will require the rights and obligations between the Financial Entity and of its ICT third-party service provider to be clearly allocated and set out in writing. DORA will require the full contract to include service level agreements and be documented as specified within the regulation. Furthermore, DORA **specifies a wide array of specific matters and provisions which will need to be included within contractual arrangements** between a Financial Entity and any **ICT third-party service providers** (including those which are not critical). If the ICT services provided by the third-party support critical or important functions, contractual arrangements with such service providers will be required to include additional contractual provisions as described in DORA. In addition, under DORA, Financial Entities and ICT third-party service providers shall consider using **standard contractual clauses introduced by public authorities for specific services** at the stage of negotiations for contractual arrangements. The above-mentioned requirements **will affect new and existing contracts alike.**

EU Presence of the 'critical' ICT third-party service providers

Under DORA, Financial Entities will **not be permitted to use services provided by critical ICT third-party service providers** established in a **non-EU state, unless** such service provider **establishes a subsidiary in the EU** state within the twelve months following such service provider's designation as 'critical' by the European Supervisory Authorities.

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

Next Steps

Financial Entities should consider taking the following initial steps in order to achieve compliance with the new regulatory requirements:

Gap analysis

Financial Entities should conduct a gap analysis of their **existing ICT-related risk and governance procedures and mechanisms** in light of the newly introduced requirements under DORA, evaluate whether they are **eligible for any exemptions** from certain requirements under DORA, determine which **procedures and mechanisms are expected to be impacted by DORA**, and plan ahead the steps to be taken in order to **ensure compliance** with the newly introduced obligations and requirements under DORA. Such gap analysis should address, among others, the **existence of the required policies, procedures, programs, protocols and tools** in place, and the **ability** of the Financial Entity **to properly assess and manage ICT-related risks**.

Contractual arrangements with ICT third-party service providers

Financial Entities should identify the **existing contracts** with service providers which will fall under the contractual arrangement requirements introduced as part of DORA. Following this step, Financial Entities should **evaluate which changes are required** to be made in such contacts, and **begin negotiating** such revisions with the relevant service providers.

Evaluating compliance of 'critical' ICT third-party service providers

Financial Entities should **assess which third-party service providers are likely to be designated as 'critical'** (e.g., cloud service providers), and contact these service providers and in order to understand their intentions and plans for compliance with requirements set out in DORA. Specifically, if such service provider does not have EU presence, Financial Entity should ensure that the existing service provider which is expected to be designated as 'critical' seeks to establish a subsidiary in the EU, or otherwise seek for an alternative.

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

ICT third-party service providers should:

Evaluating service recipients and type

evaluate **whether they are providing service to Financial Entities,** and their **likelihood to be designated as 'critical' ICT third-party service provider.** While the designation of types of entities which will be considered as 'critical' is yet to be made, it is generally considered that some service providers (e.g., cloud service providers) will likely fall under such definition. ICT third-party service providers designated as 'critical' will be subject to certain regulatory framework and will be required to be EU-based or to have a subsidiary in the EU.

As mentioned, DORA **will apply from 17 January 2025,** with **additional technical standards** and **more detailed requirements** expected to be further introduced by the competent authorities. **Covered businesses should already start getting acquainted with DORA's provisions and take actions in order to adequately prepare for compliance with its new obligations, which may require significant efforts and adjustments, including to existing procedures and contracts.**

Please feel free to contact us with any further questions or comments regarding the effect and implications of DORA, and how it may affect your compliance efforts.

HERZOG
HERZOG FOX & NEEMAN

DORA: How to Prepare

Herzog's Technology & eCommerce Regulation Department

Herzog's Technology & eCommerce Regulation Department is a recognized market leader in its field. The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions, digital platforms** and leading **self-regulatory** guidelines. This enables our team to offer **practical, holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

Technological developments in recent years are reshaping the world of **finance, payments, trading and investments.** Our department has positioned itself at the forefront of this burgeoning industry by providing a **holistic suite** of **end-to-end legal services,** to assist clients in operating their businesses in accordance with all the applicable regulatory and business considerations. We assist our clients in ensuring they have appropriate measures in place, in order to manage their **data protection and cyber risks** and to respond effectively to incidents, while mitigating potential regulatory risks. Our clients include international operators and creators in the crypto sector, financial technologies and payments providers, banks and finance intermediators.

Ariel Yosefi | Partner
Head of Technology & eCommerce Regulation
yosefia@herzoglaw.co.il

Dima Zalyalyeyev | Associate
Technology & eCommerce Regulation
zalyalyeyevd@herzoglaw.co.il

Ido Manor | Partner
Technology & eCommerce Regulation
manori@herzoglaw.co.il

Eden Lang | Associate
Technology & eCommerce Regulation
lange@herzoglaw.co.il

Ruly Ber | Partner
Technology & eCommerce Regulation
berr@herzoglaw.co.il

On Dvori | Associate
Technology & eCommerce Regulation
dvorio@herzoglaw.co.il

Dan Shalev | Partner
Technology & eCommerce Regulation
shalevd@herzoglaw.co.il

Kevin David Gampel | Associate
Technology & eCommerce Regulation
gampelk@herzoglaw.co.il

Moran Bergman | Associate
Technology & eCommerce Regulation
bergmanm@herzoglaw.co.il

Or Noy | Associate
Technology & eCommerce Regulation
noyo@herzoglaw.co.il

Mai Arlowski | Intern
Technology & eCommerce Regulation
arlowskim@herzoglaw.co.il

Oded Kramer | Associate
Technology & eCommerce Regulation
kramero@herzoglaw.co.il

Shlomo Friedman | Intern
Technology & eCommerce Regulation
friedmans@herzoglaw.co.il

Liron Adar | Intern
Technology & eCommerce Regulation
adarl@herzoglaw.co.il