BARNEA

DORA

Privacy, Cyber & AI Department

Barnea Jaffa Lande & co, Law Firm

BARNEA

DORA for Tech Vendors

What You Should Know (But Haven’t Asked)

What is DORA?

DORA (Digital Operational Resilience Act) is an EU regulation that sets rules for how financial entities manage ICT (Information and Communication Technology) risks. It covers areas like cyber resilience, incident reporting, third-party risk, and oversight of critical service providers.

Who does DORA apply to?

DORA applies to EU financial institutions (e.g. banks, insurers, investment firms, payment providers, crypto platforms) and to their ICT third-party service providers (TPPs). This includes cloud platforms, SaaS vendors, cybersecurity firms, and other tech providers to EU financial institutions.

Does DORA also apply to companies outside the EU?

Yes – if you provide ICT services to EU financial institutions, DORA may apply, regardless of where you’re based. The impact may be direct or contractual, depending on your role. Not sure where you stand? We can help you assess that.

I’m an ICT service provider working with an EU financial institution. How does DORA affect me?

Yes, in one of three ways:

- Directly, if you’re formally designated by EU regulators as a “critical ICT provider” – subjecting you to direct oversight and compliance obligations.
- Contractually, if your services are considered as supporting critical or important functions to the financial entity’s operations – in which case DORA compliance may be built into your contract with the financial entity.
- Minimally, even if not critical, financial entities still need to manage all ICT risks – so you may face lighter contractual obligations.

What are “critical services” under DORA?

Critical services are ICT services that, if disrupted, could impact the stability or resilience of the EU financial sector, not just one company. DORA uses this term when assessing whether a provider should be designated as a critical third-party provider (“CTTP”) at the EU regulatory level. This is different from services that “support critical or important functions” for individual financial entities (see further below).

What is a "critical or important function" under DORA?

It's a service or function that, if disrupted, could significantly impact a financial entity's operations or stability. Factors include the function's scale, substitutability, cross-border relevance, and operational dependency. Determining this requires a case-by-case analysis.

What kind of contractual obligations might apply?

DORA requires financial entities to include specific clauses in their contracts with ICT providers – especially those supporting critical or important functions. These may cover: Security and risk controls; incident response and reporting; audit and oversight rights; termination and exit planning and more. Obligations vary by the provider's classification and the entity's own risk assessment.

How should my company prepare?

Start by assessing whether your services are considered critical or important to the financial entity you support. This will guide the level of compliance expected of you. From there, review and align your contracts, security measures, and incident processes. Each case is different – we can help tailor the right approach.

Is DORA in effect?

Yes. DORA became fully applicable on January 17, 2025, and financial entities – along with their ICT providers – are now expected to comply. However, implementation may vary across EU countries. Some jurisdictions have adopted it more quickly or added local requirements, while others are still aligning their supervisory practices, which may affect applicability and repercussions.

What happens if we don't comply?

If you're formally classified as critical, failure to comply could lead to direct regulatory action and sanctions. Otherwise, noncompliance could result in contract penalties or termination, reputational harm or loss of business. Financial entities are under pressure to demonstrate compliance – and may stop working with providers that fall short.

Our Privacy, Cyber and AI team advises financial institutions, fintechs, and ICT providers on practical DORA compliance - covering cyber risk management, third-party oversight, contractual obligations, and incident response.
With cross-border expertise and deep regulatory insight, we help clients implement DORA efficiently and mitigate legal and operational risks.

Questions about DORA? We're here to help.

BARNEA

Privacy, Cyber & AI Team

2.6.25 0.6

Dr. Avishay Klein, Partner, Head of Department

Avishay is a leading Israeli attorney specializing in privacy, artificial intelligence (AI), and information security, and formerly served as the Data Protection Officer (DPO) of Amdocs Group. He advises organizations on complex privacy, cybersecurity, and AI regulatory matters, and is a founding member of the Israeli DPO Forum and a lecturer on law, technology, and cyber regulation.

Masha Yudashkin, Associate

Masha is a brilliant attorney with extensive experience advising public and private sector organizations on AI regulation, privacy, and data protection. She supports clients in navigating advanced regulatory frameworks such as the EU AI Act and international risk management standards, including NIST and ISO 42001, and provides legal guidance on the contractual and compliance aspects of AI system integration.

Liav Shapira, Senior Associate

Liav is a seasoned commercial attorney specializing in privacy, data protection, and cybersecurity, with extensive experience advising tech companies, financial institutions, and public bodies on local and international regulatory challenges. He serves as an outsourced Data Protection Officer (DPO), guiding organizations through compliance programs, risk assessments, and policy development under frameworks such as GDPR, DORA, CCPA, and others.

Nadine Liv, Associate

Nadine is a cyber crisis consultant and legal researcher with extensive experience in cybersecurity law, defense exports, and AI regulation. She holds a PhD (expected 2025) in Law with a focus on braincomputer interfaces, and her work bridges academia, regulatory policy, and high-stakes operational guidance during cyber crises.