Digital Operational Resilience Act For Financial **Services** (DORA) Quick Guide

simmons+simmons

What is the Digital Operational Resilience Act (DORA)?

DORA aims to achieve a **high common level of digital operational resilience** of **financial entities** in the EU.

It establishes uniform requirements for the security of network and information (ICT) systems supporting the business processes of financial entities.

The requirements applicable to financial entities include:

- ICT risk management
- Reporting of major ICT-related incidents
- Digital operational resilience testing
- Information and intelligence sharing related to cyber threats and vulnerabilities
- Measures for managing ICT third-party risk

In addition, DORA sets out:

- Requirements for contractual arrangements between ICT third-party service providers and financial entities
- Rules for the establishment and conduct of an Oversight Framework for critical ICT third-party service providers

Timeline

- DORA entered into force on 16 January 2023.
- DORA will generally become applicable as of **17 January 2025**.

Difference to EBA/ESMA/EIOPA-Guidelines

EBA/ESMA/EIOPA-Guidelines

- Addressees: authorities (*e.g.*, Federal Financial Supervisory Authority ('BaFin'))
- Aim: harmonisation of administrative practice
- Problem: not every authority implements/is under obligation

DORA Regulation

- Addressees: 'financial entities' resp. 'ICT third-party service providers' themselves
- Authorities are obliged to become active
- Extended scope of application: 'financial entities' and 'ICT third-party service providers' are to be understood very broadly

Scope

Financial entities

Among others:
- Credit institutions
- Payment institutions
- Electronic money institutions
- Investment firms
- Insurance/reinsurance undertakings
- Management companies
- Crypto-asset service providers
- Trading venues
- Crowdfunding service providers
- Data reporting service providers
- Credit rating agencies

ICT third-party service providers

'Undertaking providing ICT services'

ICT services:
'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'

To be understood broadly → Including among others:
- Cloud computing services
- Software
- Data analysis services
- Providers of data centre services

General obligations

Financial entities

- ICT risk management
- ICT-related incident reporting
- Digital operational resilience testing
- Information exchange
- Managing of ICT third-party risk

Before entering into a contractual agreement on the use of ICT services, financial entities shall carry out an assessment:
- Suitability of the ICT third-party service provider (Selection and assessment process)
- ICT service supporting a critical or important function
- Increased ICT concentration risk (for critical/important functions)?

⇒ ICT third-party service provider is not easily substitutable

⇒ Multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions (!) with the same ICT third-party service provider (or with closely connected ICT third-party service providers)

The higher the risk, the higher the requirements for ICT third-party service providers in the context of outsourcing contracts!

Obligations regarding contracts

Information security standards

Principle:
ICT third-party service providers need to comply with 'appropriate information security standards'

Contractual arrangements concerning critical or important functions:
Financial entities shall, prior to concluding the arrangements, take due consideration of the **use**, by ICT third-party service providers, of the most up-to-date and highest quality information security standards

Contractual requirements in the context of outsourcing

Principle (non-exhaustive):
Clear and complete description of all functions and services, locations (incl. data processing, storage location), Service level descriptions, provisions ensuring access, reporting incidents, termination rights

Additionally to include for ICT services supporting critical or important functions (non-exhaustive):

- Obligation to participate in financial entity's TLPT
- Unrestricted rights of access, inspection and audit by the financial entity/an appointed third party
- Exit strategy management

Providing information about contractual agreements

= Duty of the financial entities

- Maintenance of an information register in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers (regular updates required)
- At least yearly: Reporting to competent authorities on any ICT services utilised
- In a timely manner: Informing the competent authority about any planned contractual arrangements on the use of ICT services supporting critical or important functions as well as when a function has become critical or important

! Financial entities will try to pass on this compliance pressure to third-party ICT service providers (*e.g.*, in contract negotiations)

! Administrative and criminal penalties possible → Member States will lay down penalties!

! Publication of administrative penalties

Critical ICT third-party service providers

Designation

Designation by EBA, ESMA, EIOPA (supervisory authorities), according to the relevant criteria (non-exhaustive):

- Systemic character of the financial entities
- Reliance
- Degree of substitutability

Systemic Character assessed in accordance with the following parameters, *e.g.*:

- Number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider

The degree of substitutability of the ICT third-party service provider, taking into account the following parameters:

- 'Lack of real alternatives'
- 'Difficulties in relation to migrating the relevant data and workloads from the relevant ICT third-party service provider to another ICT third-party service provider, due either to significant financial costs, time or other resources that the migration process may entail, or to increased ICT risk'

If categorised as a critical ICT third-party service provider:
Strict 'monitoring framework'

Extensive Oversight Framework

Assessment of ICT services, namely among others:

- Quality of services
- Infrastructure, physical security, including data centre security
- Response and recovery plans

Issuing recommendations

Ongoing oversight

- Request for information, general investigations, inspections
- Oversight fees for critical ICT third-party service providers for 'ongoing oversight' (cost-covering & in reasonable proportion to turnover)

Imposing a periodic penalty payment, *e.g.*, if recommendations are not implemented:

- Daily penalty payment (max. 6 months) (Up to 1% of the average worldwide daily turnover)
- Disclosure to the public of every imposed periodic penalty payment

How can I prepare for DORA?

Financial entities and third-party ICT service providers need to prepare for the applicability from January 2025.

Financial entities

- ✓ Put an ICT risk management framework in place that complies with DORA
- ✓ Monitor third-party risk throughout the contractual relationship with an ICT service provider
- ✓ Ensure compliance with mandatory contractual provisions for contracts involving critical or important functions required by DORA

ICT third-party service providers

Contract Lifecycle Management:

- Which customers are subject to DORA?
- Do the contracts with them need to be adapted?
- Especially for 'critical functions': Have EBA/ESMA/EIOPA guidelines already been taken into account?

Critical ICT third-party service providers:

- Is my company likely to be categorised as a 'critical third-party ICT service provider'?
- If so, how do I best manage the associated risks?
- Comparison of DORA/existing guidelines (*e.g.*, BAIT) with own processes

Relevant contacts:

Christopher Götz, LL.M. (New York)
Simmons & Simmons LLP, Munich

Partner Digital Business

Hinal Patel
Simmons & Simmons LLP, Bristol

Partner Digital Business

Eric Le Quellenec
Simmons & Simmons LLP, Paris

Partner Corporate & Commercial

Jochen Kindermann
Simmons & Simmons LLP, Frankfurt

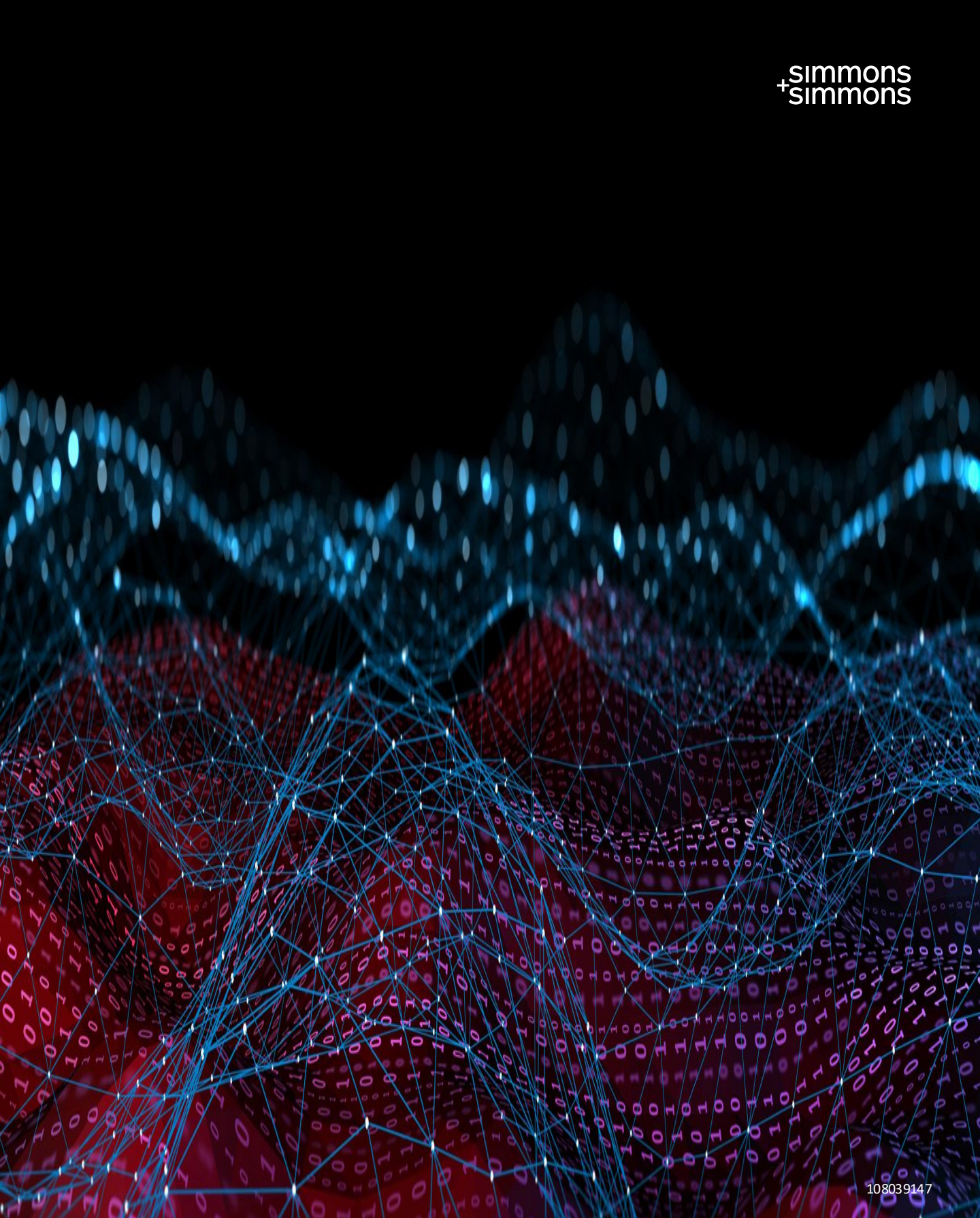
Partner Financial Markets

Camille Saettel
Simmons & Simmons LLP, Luxembourg

Counsel Digital Business

Sophie Sheldon
Simmons & Simmons LLP, London

Partner Digital Business



simmons-simmons.com

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.