BAUMGARTNER BAUMANN

Author:

Dr. Lukas Fleischer
Associate

04.04.2025

ICT third-party service providers under the DORA: contract design in the light of digital resilience

Read briefly:

From January 17, 2025, the Digital Operational Resilience Act ("DORA") will apply throughout the EU. The DORA creates a comprehensive legal framework aimed at strengthening the digital resilience of financial companies. The DORA obliges financial companies (among others) to agree specific contractual provisions with their service providers in the field of information and communication technology (so-called ICT third-party service providers, e.g. software providers). The following article examines what this can mean for service providers of financial companies.

1. ICT third-party service providers

The DORA applies primarily to financial companies, such as credit and payment institutions and insurance companies (Art. 2 para. 1 and 2 DORA). DORA places specific requirements on the design of the digital systems and processes of these companies. In addition to the assessment of digital risks (e.g. cyberattacks), this includes in particular the implementation of risk mitigation measures.

In addition to financial companies, the DORA also applies to so-called ICT third-party service providers (Section 2 (1) (u) DORA). The term “ICT third-party service provider” is formulated very broadly and aims to subject those involved in the digital transformation of the financial services industry to the provisions of the DORA. In principle, the term should therefore include all companies that continuously provide digital services or data services via ICT systems to one or more internal or external users in the financial sector (Recital 35 of the DORA), i.e. usually in particular

- Cloud computing providers: Companies that provide storage and computing resources over the internet.
- Software providers: Companies that develop or provide software solutions for financial companies.
- Data analytics services: Companies that perform data processing and analysis for financial institutions
- Data centers: Companies that provide physical infrastructure for the storage and processing of data.

2. Contractual content in accordance with Art. 30 DORA

The DORA contains special obligations for financial companies that must be observed when working with or commissioning third-party service providers. A central task of the acting financial company is to draw up a contractual agreement with the commissioned ICT third-party service provider (Art. 30 DORA). The financial company must ensure that the rights and obligations of both parties are clearly defined and set out in writing (Art. 30 para. 1 DORA). For the design of the contractual agreement, Art. 30 para. 2 DORA contains minimum provisions that must be implemented each time an ICT third-party service provider is commissioned by the financial company. These include in particular

Service description: A clear definition of the ICT services (including the conditions for subcontracting).

Data protection: Provisions on availability, authenticity, integrity and confidentiality with regard to data protection (including the protection of personal data).
Assistance and cooperation: The obligation of the ICT Third Party Service Provider to assist the Financial Company in the event of an ICT Incident related to the ICT Service of the ICT Third Party Service Provider. The obligation of the third-party ICT service provider to cooperate with the supervisory authorities responsible for the financial undertaking.
Termination clauses: termination rights and minimum notice periods for the termination of contractual agreements.

If the contracted ICT third-party service provider supports the financial company in critical or important functions, additional provisions must be included in the contractual agreement in addition to the minimum provisions (Art. 30 para. 3 DORA). A function is critical or important if, for example, its failure significantly impairs the financial performance of the financial undertaking or its business operations. If a critical or important function exists, the following contract contents in particular must also be regulated:

ICT security: The obligation of the third-party ICT service provider to implement and test contingency plans. The obligation of the ICT third-party service provider to develop and maintain measures, tools and guidelines for ICT security.

- Penetration tests: The obligation of the ICT third-party service provider to support the financial company with threat-led penetration tests (TLPTs).
- Monitoring and access rights: The right of the financial company and the competent authority to gain unrestricted access to the business premises of the ICT third-party service provider in order to carry out inspections and audits.
- Exit strategy: Arrangements to ensure business continuity in the event of termination of the contract or a change of the ICT third-party service provider.

3. To-Dos for Businesses

As Art. 30 DORA is only directly aimed at financial companies, ICT third-party service providers are not automatically obliged to revise existing (service) contracts. However, ICT third-party service providers should prepare themselves for the fact that their customers from the financial sector (financial companies) will confront them with the implementation of the regulations set out in DORA. Accordingly, companies that provide services for financial companies are well advised to ask themselves the following contractual questions:

- As a service provider, does the company fall within the definition of an ICT third party service provider with the service offered?
- What type of ICT service does the company provide? Does the company support an important or critical function of the financial institution or does the service only concern a “non-critical” function at the financial institution?
- Do the existing contracts meet the legal requirements that DORA places on the ICT service to be provided?
- What contractual provisions should be concluded with the company's own (sub)processors in order to avoid a liability risk vis-à-vis the financial company commissioning the service?