FINLAW

Threats, Incidents, and Attacks Under DORA

What Financial Companies Need to Know

(10.11.2025)

FINLAW

1 Introduction to DORA and Core Objectives

- Regulation (EU) 2022/2554 – better known as **DORA** – has been compulsory for financial companies since January 17, 2025.
- A key objective of the regulation is to **strengthen the digital operational resilience** of the financial sector.
- DORA aims to create clear structures for dealing with ICT risks.
- The regulation makes a precise distinction between **threats**, **incidents**, and **attacks**.
- Precise classification is of central importance not only for compliance but also for the strategic orientation of ICT risk management.

2 Defining Threats (Potential Sources of Danger)

- DORA broadly divides terms into two categories: **threats** (which have the potential to cause damage) and **incidents/attacks** (the actual events that have caused or are causing damage).
- Threats refer to possible circumstances or actions that could affect network and information systems (ICT).
- A **cyber threat** (Art. 3 No. 12 DORA) is a possible circumstance, event, or action that could harm, disrupt, or otherwise affect network and information systems.
- A **significant cyber threat** (Art. 3 No. 13 DORA) indicates the potential to cause a serious ICT-related incident.
- Threats as potential sources of danger are primarily to be analyzed internally.

3 Defining Incidents and Attacks (Actual Events)

- An **ICT-related incident** (Art. 3 No. 8 DORA) is the most general category of a negative event in the ICT sector.
- It is an unplanned event that compromises the security of network and information systems.
- The incident must have an adverse impact on the availability, authenticity, integrity, or confidentiality of data or on the services provided.
- ICT-related incidents are subdivided into **serious ICT-related incidents** and **serious payment-related operational or security incidents**.
- A **cyberattack** (Art. 3 No. 14 DORA) is a malicious ICT-related incident resulting from an attacker's attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or use of an asset.

4 Obligations for Threats (Internal & Voluntary Reporting)

- There is **no external reporting obligation** for cyber threats as a general threat category.
- Information gained from threats is used primarily for internal analysis and further development of digital operational resilience.
- Reporting a significant cyber threat to the competent authorities is **voluntary** under Article 19(2) DORA.
- Financial companies may share this information if they consider the threat to be relevant to the financial system, service users, or customers.
- DORA focuses on proactive integration into risk management and voluntary information sharing in the event of threats.

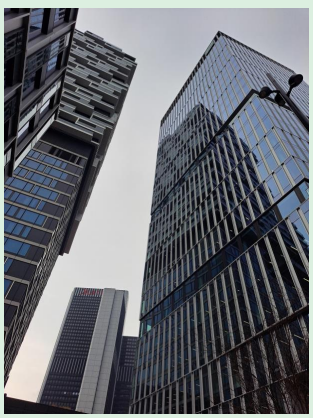
5 Obligations for Serious Incidents (Mandatory Reporting & Review)

- ICT-related incidents and cyberattacks only trigger an external reporting obligation if they reach a certain level of severity, i.e., if they are classified as **serious**.
- Financial companies must report serious ICT-related incidents to the competent authority (Art. 19 (1) DORA).
- Certain institutions must also report serious payment-related operational or security incidents (Art. 23 DORA). This specific obligation replaces the corresponding reporting obligations under PSD2 to avoid duplication of requirements.
- Following disruptions resulting from serious ICT-related incidents, financial companies must provide for subsequent reviews of the incident.
- These reviews should investigate the causes and identify improvements to ICT processes or the ICT business continuity policy.

Contacts

Anton Schröder

German Attorney at Law,
Associate at FIN LAW



FIN LAW

Auffenberg und Uhink
Partnerschaftsgesellschaft
von Rechtsanwälten mbB

Senckenberganlage 19
60325 Frankfurt am Main

E. info@fin-law.de

I. https://fin-law.de

T. +49 69 87 000 1320