SQUIRE PATTON BOGGS

# DORA Regulation

Europe – February 2024

## Overview

The Regulation (EU) 2022/2554 of the European Parliament and of the European Council of 14 December 2022, on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA), came into force on 17 January 2023, and shall be applied from 17 January 2025 onwards by the EU member states.

The legal act is intended to improve the digital security and operational resilience of EU financial companies and their information and communication technology (ICT) third-party service providers across the EU, and to create a uniform supervisory framework throughout the EU. The aim is to reduce vulnerability to cyber threats and ICT disruptions across the entire IT supply chain of the financial sector.

The EU-wide harmonisation of national regulations for the security of IT systems in the financial sector is intended to strengthen the European financial market against cyber-risks and ICT incidents. The operational stability of the EU's financial system is to be guaranteed even in the event of serious disruptions.

Furthermore, the focus is on the creation of a European supervisory body for critical IT service providers. Three European supervisory authorities (ESAs) are responsible for their introduction and monitoring. Specifically, these are the European Insurance and Occupational Pensions Authority (EIOPA), the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA).

DORA is not only of great interest to financial entities themselves, but also to IT service providers in the financial sector – particularly due to the new powers of the ESAs (contract termination claims/enforcement and fines). For critical third-party IT providers and subcontractors, for example, DORA stipulates that only service providers and suppliers seated in the EU are permitted.

The regulation is further defined by regulatory technical standards (RTS) and implementing technical standards (ITS). These should be drawn up with a deadline of 12 to 18 months so that they can then be implemented nationally as DORA accompanying legislation or as IT implementation. These Level 2 legal acts are planned for January and July 2024 respectively, so that the implementation of DORA within the EU member states should be possible by 17 January 2025, at the latest. The publication of the first series of RTS/ITS is planned for the first half of 2024, including those on the ICT Risk Management Framework, operational security, classification of ICT incidents, and ICT third-party risk management. The publication of the second series of RTS/ITS is planned for the second half of 2024, including those on the reporting of ICT incidents, criteria, methodologies, and requirements for testing digital operational resilience and specifications for the design of sub-outsourcing arrangements.

## Five Main Areas of DORA

### ICT Risk Management

The first area comprises the regulations on ICT risk management (Art. 5- 16 DORA). This is probably the most relevant part of the regulation for financial entities. It legitimises the establishment of a management body as well as various provisions for ICT risk management and governance. It also specifies the different technical requirements (ICT requirements) that need to be met. Financial entities are required to set up a management body. In the case of banks, the tasks of this management body are handled by the executive board. The management body is responsible for defining, approving, overseeing and implementing all arrangements related to the ICT risk management framework (Art. 5 (2) DORA).

Furthermore, the management body's tasks include managing the financial entity's ICT risk (Art. 5 (2), (a) DORA), as well as setting up and approving the digital operational resilience strategy (Art. 5 (2), (f) DORA). Also, the management body needs to approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications (Art. 5 (2), (f) DORA).

To keep up with the latest developments and thus provide sufficient knowledge and skills in terms of understanding and managing ICT risks, members of the management body are obligated to receive training in those areas on a regular basis (Art. 5 (4) DORA).

The obligations also include a strict control of the programmes being used to store and exchange data, especially when it comes to systems that are provided by a third-party service provider.

Notably, only authorised software should be installed, either for exchanging or storing data (Art. 11 (2), (c) RTS). Here, the management body not only needs to ensure that all the criteria to perform the critical assessment of information assets and ICT assets supporting business functions are met (Art. 8 (1) DORA), but also that teleworking and the use of private endpoint devices should not threaten the ICT security at any time (Art 11 (2), (j) RTS). Further, it must be ensured that an automated vulnerability scanning is performed at least once a week (Art. 10 (2), (b) RTS). This applies to the entities' internal IT systems, as well as to the third-party service provider. Vulnerabilities must be reported and patched; if no patches are available, financial entities shall identify and implement other mitigation measures (Art. 10 (2), (c- f) RTS). In addition, the management body needs to ensure that data is always encrypted – at rest, in transit and, where relevant, in use (Art. 6 (2), (a) RTS). Finally, in case of a cyberattack, measures to temporarily isolate subnetworks, networks and devices need to be implemented (Art. 13 (1) (j) RTS) to guarantee the systems' stability.

## ICT-related Incident Management

The second area (Art. 17 – 23 DORA) focuses on ICT-related incident management, and how incidents need to be classified and reported in detail. Financial entities are obliged to develop a reliable procedure for recording and classifying of serious incidents (Art. 17 (1) DORA). ESA has developed specified criteria for this purpose and has also developed harmonised standard templates for preparing reports on incidents at all stages (Art. 20 DORA). A distinction must be made here between an obligation to report incidents that have occurred (Art. 19 DORA) and an optional reporting option for threats or cyberattacks that have not led to an actual incident.

## Operational Resilience and Risk Management

The third area (Art. 24 – 27 DORA) focuses on the testing of digital operational resilience and risk management. Financial entities are obliged to carry out annual basic tests of their ICT systems and tools to identify and implement necessary measures against ICT risks (Art. 24 (6) DORA). Furthermore, regular advanced threat-driven penetration tests for ICT services that affect critical functions must be carried out with the mandatory participation and cooperation of third-party providers of ICT services (Art. 26 DORA). The framework conditions to be met for these advanced tests are set out in Art. 26 and Art. 27 of DORA.

## Management of Third-party Risk

The fourth area (Art. 28 – 44 DORA) focuses on the management of third-party risk; this includes the general principles as well as the structure of an oversight frame network for critical service providers. There is an obligation of financial companies to ensure the monitoring of risks arising from the use of third-party ICT providers, as well as to report a complete list of all outsourced activities (Art. 28 DORA), report at least certain functions and characteristics (Art. 30 DORA), and comply with special reporting obligations, especially in relation to third-party services (Art. 29 DORA). In addition to the management within the entity, a higher-level supervisory authority (Lead Overseer) is also responsible for critical service providers (Art. 32 DORA). The costs for this must be borne by the critical service provider (Art. 43 DORA). Which service providers are critical service providers must be determined based on criteria within the DORA Regulation.

## Exchange of information

The fifth area (Art. 45 – 56 DORA) focuses on the exchange of information, especially on behalf of cybersecurity, between the different financial entities, as well as on the possible sanctions in case of noncompliance with the regulations. Art. 45 et seq. of the DORA Regulation sets out various requirements as to how the exchange of information must take place. Specifically for Germany, however, it can be said that some steps have already been taken toward regulating cybersecurity in this area through German legislation. Through MaRisk,[1] for example, there are already minimum-security requirements for services that are provided by ICT service providers. These are further specified by BAIT,[2] KAIT,[3] VAIT[4] and ZAIT.[5] Depending on how many of these German regulations have already been fulfilled by financial entities, it may not be necessary to introduce further requirements in order to comply with DORA.

The establishment and implementation of new processes or ICS management systems, workflows with documentation evidence and management and the adaptation of the "written rules", to name but a few, are highly relevant here. Furthermore, Art. 50 et seq. of DORA lists sanctions that can be imposed on financial companies and or third-party ICT service providers in the event of noncompliance with the regulation, for example.

## Conclusion

If DORA requirements are not implemented by the companies or IT service providers within this period and audits by the supervisory authorities from 2025 onwards come to this conclusion, the ESAs can impose fines of up to 1% of daily global turnover. In addition, financial entities can be requested to terminate contracts with service providers due to noncompliance with the requirements, which means that replacement suppliers must always be available (Art. 35 (6,8) DORA).

1 MaRisk is an abbreviation referring to the minimum requirements for risk management, a circular by the German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* (BaFin)) providing concepts for risk management of banks, insurances and other companies financially trading in Germany.

2 The German Banking Supervision Requirements (BAIT) are administrative instructions published in a circular by BaFin for the secure design of IT systems and the associated processes and related requirements for IT governance in German credit institutions.

3 The Capital Management Supervisory Requirements (KAIT) for IT are administrative instructions published in a circular by BaFin for the secure design of IT systems and the associated processes and related requirements for IT governance at German capital management companies.

4 The Insurance Supervisory Requirements (VAIT) for IT are administrative regulations published in a circular by BaFin for the secure design of IT systems and the associated processes and related requirements for IT governance at German insurance companies.

5 The Payment Services Supervisory Requirements of Payment and Electronic Money Institutions (ZAIT) for the IT are administrative instructions published in a circular from BaFin for the secure design of IT systems and the associated processes and related IT governance requirements for German financial institutions.

## Applicability to Third-country Financial Entities

The basic prerequisite for the possibility of an obligation to comply with DORA is to be active as a financial entity (Art. 2 DORA) within the EU. The term "financial entity" is defined in Art. 2 (2) of DORA and includes credit institutions and payment institutions. Art. 3 No. 31 of DORA defines "credit institution" as a credit institution within the meaning of Art. 4 (1), No. 1 of Regulation (EU) No. 575/2013 of the European Parliament and of the council. Art. 3 No. 35 of DORA defines "payment institution" as a payment institution within the meaning of Art. 4 No. 4 of Directive (EU) 2015/2366.

If a financial entity operates a branch or subsidiary within Germany, it is subject to both German law and EU law, meaning that the provisions of DORA must be complied with. Furthermore, in these cases, parent companies based in non-EU countries can also be obliged to exchange information with the ICT supervisory authority (Art. 36 DORA).

There is a lot of uncertainty here. DORA is likely to cover both financial entities authorised in the EU and financial entities that are not authorised in the EU but provide services in the EU, whether authorised or not.

## Third-party ICT Service Providers

In general, a distinction must be made between critical and noncritical third-party ICT service providers. In general, the financial entities are responsible vis-à-vis the EU for ensuring that the ICT third-party service providers comply with the regulations (Art. 28 (1) DORA). The financial entities therefore have extensive monitoring obligations with regard to the activities of the third-party ICT service providers. The objective is to ensure that appropriate information security standards are being complied with (Art. 28 (5) DORA).

### Noncritical ICT Third-party Service Providers

To fulfil these obligations, the financial entities are obliged to stipulate certain compliance requirements in the contracts with the third-party service providers.

#### Minimum Requirements

The minimum requirements for these compliance conditions are set out in Art. 30 of DORA and include the following:

- Clear and complete description of all functions and ICT services offered by the ICT third-party service provider
- Locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations
- Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data
- Provisions on ensuring access, recovery and return in an easily accessible format of personal and nonpersonal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements
- Service level descriptions, including updates and revisions thereof
- Obligation to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs
- Obligation to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them
- Termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities
- Conditions for the participation in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Art. 13(6) of DORA.

#### Annual security testing

In addition, annual security testing must be carried out to be prepared for ICT-related incidents, to identify vulnerabilities, deficiencies and gaps in digital operational resilience, and to take timely remedial action (Art. 24 (1) DORA). These audits shall include (in accordance with the criteria set out in Art. 4(2) of DORA) vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scans of software solutions, source code reviews where feasible, scenario-based testing, compatibility testing, performance testing, end-to-end testing, and penetration testing (Art. 25 (1) DORA). The frequency of audits and inspections and the areas to be audited should be determined in accordance with generally accepted auditing standards in line with any supervisory instruction on the application and inclusion of such auditing standards (Art. 28 (6) DORA).

#### Termination

Contractual arrangements for the termination of the use of third-party ICT services should also be included (Art. 28 (7) DORA).

#### GDPR

Compliance with EU data protection rules and the effective enforcement of the law in that third country must be ensured (Art. 29 (2) DORA).

#### Subcontracting

In the case of subcontracting, the ICT third-party service provider must continue to ensure that these subcontractors also comply with the regulations. This is the only way to ensure comprehensive security (Art. 29 (2) DORA).

## Critical ICT Third-party Service Providers

Under certain conditions, service providers can be classified as critical providers.[6] In addition to the obligations already mentioned, they are subject to further obligations. On the one hand, there are further obligations toward the financial entities, and, on the other hand, additional obligations toward a supervisory body of the EU arise.

### Further Obligations Toward Financial Entities

In addition to the elements already listed, the contractual arrangements on the use of ICT services supporting critical or important functions shall at least include the following (Art. 30 DORA; Art. 8, 9 RTS):

- Full service-level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels, to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met
- Notice periods and reporting obligations to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels
- Requirements to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework
- Obligation to participate and fully cooperate in the financial entity's threat-led penetration testing (TLPT) as referred to in Art. 26 and 27 of DORA
- Right to monitor, on an ongoing basis, the performance, which entails the following:
  - Unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies
  - Right to agree on alternative assurance levels if other clients' rights are affected
  - Obligation to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party
  - Obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits
- Exit strategies, in particular the establishment of a mandatory adequate transition period:
  - During which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring
  - Allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided
- There must also be exit strategies in the event of contract termination so that a seamless switch to another provider is possible without any disadvantages for the financial entities (Art. 28 (8) DORA). It should be ensured that financial entities are able to exit contractual arrangements without:
  - Disruption to their business activities
  - Limiting compliance with regulatory requirements
  - Detriment to the continuity and quality of services provided to clients

  Exit plans shall be comprehensive, documented and sufficiently tested and reviewed periodically.

6 According to Art. 31 (2) DORA, if

1. The systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large-scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the relevant ICT third-party service provider provides services
2. The systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider, assessed in accordance with the following parameters:
   a. The 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
   b. The interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities, including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities
3. The reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly or indirectly, through subcontracting arrangements
4. The degree of substitutability of the ICT third-party service provider, taking into account the following parameters:
   a. the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity
   b. Difficulties in relation to partially or fully 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 or other operational risks to which the financial entity may be exposed through such migration

## Obligations Toward the EU Supervisory Body

The critical service provider is also subject to the supervision of the EU supervisory body (Oversight Forum). Once a year, the Oversight Forum compiles the results of the investigations and inspections, to be able to use them to continuously advance cybersecurity. The Oversight Forum also determines which ICT service providers may qualify as new critical service providers; ICT service providers can also be demoted as no longer critical. As part of this process, the Oversight Forum publishes a list of all critical service providers, which is publicly accessible.

### Control Rights

The Lead Overseer, as part of the Oversight Forum, has various control rights toward the critical ICT service provider.

- Lead Overseer has the power to request all relevant information and documentation. This is further specified in Art. 37 of DORA and includes all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities.
- Lead Overseer can conduct general investigations and inspections. The general investigation is specified in Art. 38 of DORA and includes the overseer's power to examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored; take or obtain certified copies of, or extracts from, such records, data, documented procedures and any other material; summon representatives of the critical ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers; interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation; request records of telephone and data traffic.
- The inspection (Art. 39 DORA) authorises the Lead Overseer to enter into, and conduct all necessary onsite inspections on, any business premises, land, or property of the ICT third-party service providers, such as head offices, operation centres and secondary premises, as well as to conduct off-site inspections. This includes the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of ICT services to financial entities.
- These options are available for all facilities in the EU as well as in third countries (Art. 36 DORA). On this basis, the Lead Overseer can make recommendations. If ICT service providers do not follow these recommendations without substantiated justification, or if ICT service providers do not close possible security gaps found by the Lead Overseer, the overseer may impose penalties. These are listed in Art. 35 (6) of DORA below and can lead to a penalty payment in the amount of up to 1% of the daily turnover per day.
- Furthermore, it is possible to suspend ICT service providers that can or could pose a security risk for a period or to prohibit cooperation with them altogether (Art. 42 DORA).

## Conclusion

All in all, DORA establishes very strict rules that must be complied with if an ICT service provider, whether based in the EU or not, wishes to offer its services in the EU. Service providers that are classified as critical service providers must be prepared not only to comply with many rules regarding their dealings with financial entities, but also to be almost completely transparent with the EU Lead Overseer.

## Contact

**Dr. Andreas Fillmann**
Partner
T +49 69 17392 423
E andreas.fillmann@squirepb.com