YPOG Briefing

Countdown DORA: 15 Key Points of the Regulation on Digital Operational Resilience in the Financial Sector

September 12, 2024

*With the Digital Operational Resilience Act ("DORA") - Regulation (EU) 2022/2554 (available **here**), the EU has established a legal framework to strengthen the stability, security and resilience of digital services in order to protect consumers and the financial sector from cyber threats. DORA applies to financial entities but also to companies that provide IT services to them, in particular cloud providers. These companies must ensure that they implement the requirements of DORA by January 2025 at the latest in order to avoid being fined under DORA. This includes, in particular, maintaining an effective defence against cyber threats, establishing mechanisms to respond to security incidents and ensuring business continuity. Below, 15 key points of DORA are presented to give companies an overview of whether DORA is applicable to them, what its requirements are and what to consider regarding its implementation.*

1. **From when does DORA apply and which additional regulations were published in connection with DORA**?
   DORA came into force on 16 January 2023 and will be fully applicable from 17 January 2025. As additional guidance for the implementation and realization of DORA, the European Supervisory Authorities EBA, ESMA and EIOPA (together the "ESAs") have published supplementary standards which contain specifications on certain topics in the form of regulatory technical standards (RTS), implementing technical standards (ITS) and guidelines. Furthermore, the European Commission has adopted specifying delegated acts. An overview of the published RTS, ITS, guidelines, and delegated acts can be found **here**. In addition to DORA, a DORA Amending Directive was published at the same time with the aim of keeping sectoral European directives consistent with the requirements of DORA. For example, Threat Led Penetration Tests ("TLPT") were included in the SREP process of the Capital Requirements Directive (CRD) under DORA. The DORA Amending Directive amends the European Directives 2009/65/EC (UCITS Directive), 2009/138/EC (Solvency II), 2011/61/EU (AIFM Directive), 2013/36/EU (Capital Requirements Directive; CRD), 2014/59/EU (Resolution Directive), 2014/65/EU (MiFID II), (EU) 2015/2366 (PSD II) and (EU) 2016/2341 (IORP II Directive).

2. **What is the aim of DORA?**
   The primary aim of DORA is to protect the digital operational stability and IT security of financial entities from serious disruptions that may occur in the context of information and communication technologies ("ICT") and to maintain their business continuity across the EU on an ongoing basis. In particular, the implementation of DORA should enable financial entities to defend against cyber-attacks, mitigate structural risks such as those arising from the concentration of ICT in the hands of a few third-party providers, and address technical complications that may affect operational stability.

3. **To which companies is DORA applicable?**
   DORA applies to companies and institutions operating in the EU financial and insurance sector from a total of twenty areas of activity listed in Art. 2 para. 1 lit. (a)-(t) DORA (so called "financial entities").

These include (a) credit institutions, (b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366, (c) account information service providers, (d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC, (e) investment firms, (f) crypto-asset service providers as authorized under the so called "Regulation on markets in crypto-assets" and issuers of asset-referenced tokens, (g) central securities depositories, (h) central counterparties, (i) trading venues, (j) trade repositories, (k) managers of alternative investment funds, (l) management companies, (m) data reporting service providers, (n) insurance and reinsurance undertakings, (o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, (p) institutions for occupational retirement provision, (q) credit rating agencies, (r) administrators of critical benchmarks, (s) crowdfunding service providers, and (t) securitization repositories.

In addition, according to Art. 2 para. 1 lit. (u), DORA applies to companies that are not financial entities themselves but provide IT services to financial entities (so-called "ICT third-party service providers"), such as cloud providers. However, a large number of the DORA provisions are not applicable to microenterprises (i.e. financial entities that employ fewer than 10 persons and whose annual turnover or balance sheet total does not exceed EUR 2 million) or are only applicable in a limited manner.

However, the following entities listed in Art. 2 para. 3 DORA are not covered by DORA: (a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU, (b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC, (c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total, (d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU, (e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises, and (f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

4. What are the main provisions of the DORA?

The main DORA provisions are contained in Chapters II-VII DORA and concern the obligation to establish and maintain effective ICT risk management (Chapter II DORA), the effective management, classification and reporting of ICT-related incidents (Chapter III DORA), the regular testing of digital operational resilience (Chapter IV DORA), the management of ICT third-party risk (Chapter V Section I DORA), the regulatory supervision and sanctioning of critical ICT third-party service providers (Chapter V Section II DORA), and the competences and obligations of competent authorities (Chapter VII DORA).

5. What requirements does DORA place on ICT risk management?

Financial entities are required to establish and annually (for microenterprises "regularly") review and document a comprehensive internal governance and control framework to effectively address ICT risks. Art. 5 para. 2 DORA describes in detail what is to be implemented within such ICT risk management framework. The definition, approval, oversight, and responsibility for the implementation of all arrangements related to the ICT risk management is the responsibility of the management body of the financial entity. Financial entities, other than microenterprises, shall also establish an independent control function regarding the monitoring and management of ICT risks. To specify the requirements for the implementation of an ICT risk management framework, the ESAs have published the "RTS specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework" (available **here**).

6. How to deal with ICT-related incidents?

Financial entities must establish procedures and processes for identifying, handling, classifying and reporting ICT-related incidents as early as possible. ICT-related incidents that are classified as major in accordance with the criteria in Art. 18 para. 1 DORA must be reported to the respective competent supervisory authority using a three-stage reporting procedure. Financial entities must also notify their clients immediately after becoming aware of the serious ICT-related incident if it has an impact on the financial interests of the clients. Cyber threats that are categorized as significant pursuant to the criteria in Art. 18 para. 2 DORA must also be documented by financial entities, although reporting in this regard is voluntary. For the purpose of defining such incidents, the ESAs have published the "RTS specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents" (available **here**). Specifications regarding the reporting of ICT-related incidents are contained in the ESAs' "RTS on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents" (available **here**) and the "ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat" (available **here**).

7. What are the requirements for testing digital operational resilience?

Financial entities, other than microenterprises, must establish a robust and comprehensive testing programme to assess their preparedness to handle ICT-related incidents, identify weaknesses, deficiencies and gaps in digital operational resilience and implement corrective actions promptly. Testing shall be conducted by independent internal or external parties and shall occur at least annually for ICT systems or applications that support critical or important functions. A selection of tests to be considered is listed in Art. 25 para. 1 DORA. According to Art. 26 DORA, certain financial entities are additionally required to conduct Threat Led Penetration Tests ("TLPT") at least every three years. The requirements for these tests were specified by the ESAs in the "RTS specifying elements related to threat led penetration tests" (available **here**).

8. What are DORA's requirements for ICT third-party risk management and contractual arrangements with ICT third-party service providers?

Except for microenterprises, ICT third-party service providers are required to establish and regularly review an ICT third-party risk policy and a guideline for the use of ICT third-party services. In this context, the ESAs published the "RTS specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers" (available **here**). To effectively manage the ICT third-party risk, financial entities must, according to Art. 28 para. 3 DORA, keep an up-to-date register of information. Specifications in this regard are contained in the ESAs' "ITS on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by the ICT third-party service providers" (available **here**). The register of information should contain up-to-date information on all outsourced ICT processes, the corresponding contractual arrangements and the categorization as critical/important or non-critical/non-important function and must be made available to the competent authorities in full or in part, if requested. In addition, financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided. Financial entities must also notify the competent authorities in a timely manner of any planned contractual arrangement for the use of ICT services supporting critical or important functions as well as when a function has become critical or important.

Before entering into a contractual agreement with an ICT third-party service provider, financial entities must conduct a risk analysis regarding the ICT third-party service provider on the basis of the criteria set out in Art. 28 para. 4 and para. 5 DORA. Regarding contract negotiations with ICT third-party service providers, financial entities need to ensure that the frequency of audits and inspections as well as the areas to be audited are determined in advance. In addition, it must be contractually ensured that the financial entity is granted termination rights for the cases mentioned in Art. 28 para. 7 DORA and that appropriate exit strategies are provided for in the event of termination of the contractual relationship in the case of critical or important functions. Finally, Art. 30 DORA provides for further essential contractual provisions to be considered in the context of contractual agreements between financial entities and ICT third-party service providers, including those relating to the admissibility and conditions of subcontracting. For this purpose, the ESAs have published the "RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions" (available **here**).

9. How and by whom are ICT third-party service providers supervised under the DORA?

The ESAs review ICT third-party service providers based on criteria specified in Art. 31 para. 2 DORA and classify them as "critical" if necessary. To specify the criteria to be considered in tis regard, the European Commission has published the "Delegated Regulation specifying the criteria for the designation of ICT third-party service providers as critical for financial entities" (available **here**). For each critical ICT third-party service provider, one of the ESAs is appointed as the "lead overseer". The powers of the lead overseer under Art. 35 para. 1 DORA include (a) the right to request all relevant information and documentation it deems necessary for the performance of its duties, (b) to conduct general investigations and (on-site) inspections, (c) to request reports upon completion of oversight activities, and (d) to issue recommendations, such as on ICT security and quality requirements or on subcontracting.

10. What sanctions does DORA provide against ICT third-party service providers in the event of violations?

To enforce its powers under Art. 35 para. 1 lit. (a)-(c) DORA, the lead overseer may impose an administrative penalty payment on critical third-party ICT service providers of up to 1% of the average daily worldwide turnover of the critical ICT third-party service provider in the preceding business year. The periodic penalty payment will be imposed daily until compliance is achieved, but for no longer than six months. Penalty payments imposed are generally published by the lead overseer. Regarding a recommendation according to Art. 35 para. 1 lit. (d) DORA, critical ICT third-party service providers shall, within 60 calendar days, either notify the lead overseer of their intention to follow the recommendation or provide a reasoned explanation for not following such. The lead overseer will publicly disclose where a critical ICT third-party service provider fails to notify the lead overseer in accordance with the DORA requirements or where the explanation provided by the critical ICT third-party service provider is not deemed sufficient. Furthermore, in such a case, the competent national authorities shall also inform the financial entities concerned and may require them to temporarily suspend the use of the respective ICT third-party service provider in whole or in part or to terminate the relevant contractual relationship in whole or in part.

11. How and by whom are financial entities supervised under DORA?

The responsibility of the authorities for the respective financial entities follows from Art. 46 DORA. The competent authorities have all supervisory, investigative and sanctioning powers necessary to fulfil their duties under DORA. Pursuant to Art. 50 para. 2 DORA, the powers include at least (a) accessing and obtaining or making copies of documents or data in any form that the competent authority considers

relevant for the performance of its duties, (b) carrying out on-site inspections or investigations, and (c) requiring corrective and remedial measures for breaches of the requirements of DORA.

12. What penalties does DORA provide for against financial entities in the event of violations?

According to Art. 50 para. 3 DORA, the EU member states must determine appropriate administrative sanctions and remedies for violations of the DORA and ensure their effective implementation. These penalties and measures must be effective, proportionate, and dissuasive. Administrative penalties are promptly published by the competent authority on its official websites in accordance with Art. 54 DORA. While DORA does not specify criminal penalties for infringements, EU member states are free to provide for such penalties in their national law.

13. To what extent do the DORA provisions differ from the provisions already in force in Germany?

The content of the DORA provisions is largely congruent with the national and European provisions for the risk management of cyber and IT risks already applicable to the German finance and insurance sector, in particular MaRisk, BAIT, ZAIT, VAIT, KAMaRisk, KAIT and the EBA and ESMA guidelines on outsourcing to cloud providers. Nevertheless, the DORA provisions go into more detail in some cases or deviate from the currently applicable provisions. For example, DORA requires the establishment of a new independent control function for the management and monitoring of ICT risk. The requirements for testing digital operational resilience are also specified and tightened by requiring extended tests based on TLPT. In addition, DORA's requirements for the content of contractual arrangements with third-party ICT service providers exceed the requirements of the current regulations in some areas. For some financial entities, e.g. asset management companies, the reporting system for security incidents is also new. Furthermore, the scope of application of DORA is much broader than the provisions currently applicable to the German finance and insurance sector, as DORA directly applies to more companies (in particular ICT third-party service providers) and does not differentiate between outsourcing and other third-party procurement. Finally, it should be emphasized that DORA, unlike the provisions currently in force, explicitly assigns the overall responsibility for non-compliance with the DORA to the management body of the financial entity, who must actively keep its ICT risk knowledge and skills up to date and participate in regular ICT-related training to understand and assess ICT-risks and their impact.

14. How does DORA relate to existing provisions and the NIS-2 Directive?

In relation to the existing provisions at EU level and the NIS-2 Directive, that was published on 27. December 2022 and must be implemented into national law by 27. October 2024, DORA is to be considered lex specialis according to its recital 16 and therefore takes precedence. In areas where the provisions of NIS-2 are more specific than those of DORA, the NIS-2 provisions apply supplementary. National regulations and requirements, such as BAIT, must be adapted so that they are consistent with the DORA requirements, although specific national characteristics may remain.

15. What should affected companies do to effectively implement the requirements of DORA?

Financial entities and ICT third-party service providers should carry out a GAP analysis of their existing processes, internal documentation and contractual arrangements with ICT third-party service providers. Identified gaps should be closed by implementing the internal processes identified as missing in the gap analysis and by drafting new or adapting existing guidelines and documentation as quickly as possible, at the latest by January 2025. In addition, existing contracts between financial entities and third-party ICT service providers should be renegotiated and updated so that they adequately reflect the DORA requirements. Particularly ICT third-party service providers should make adjustments to their standard contracts and prepare DORA supplementary agreements that they can offer to financial entities as an addendum to

their contractual arrangements to enable them to comply with DORA requirements in relation to contractual arrangements with ICT third-party service providers. In addition to the DORA requirements themselves, financial entities and ICT third-party service providers should pay particular attention to the ESAs' specifications in the form of RTS, ITS and guidelines, as these contain practical instructions for implementing the DORA requirements. The German supervisory authority BaFin (*Bundesanstalt für Finanzdienstleistungsaufsicht*) offers further assistance in its supervisory notices on DORA and other publications, which can be found on the BaFin website (available **here**).

Conclusion: The implementation of the DORA requirements is a challenge for many financial companies and IT service providers operating in the financial sector, which must be resolved as quickly as possible. We will be happy to support you with legal issues relating to this topic.

Your contacts at YPOG:

Dr. Lutz Schreiber
Partner, Hamburg
IP/IT/Data Protection

+49 406077281 234
+49 151 40229483
lutz.schreiber@ypog.law

Sara Apenburg
Partner, Hamburg
IP/IT/Data Protection

+49 40 6077281 237
+49 151 40229489
sara.apenburg@ypog.law