YPOG Briefing:

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

27 November 2023

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**?
   DORA came into force on 16 January 2023 and will be fully applicable from 17 January 2025.

2. **What is the aim of DORA?**
   The primary objective 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 authorised 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) securitisation repositories.
   In addition, according to Art. 2 para 1 lit. u), DORA applies to companies that are no 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.

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 regulatory supervision and sanctioning of financial entities (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 with regard to ICT risk management.

6. How to deal with ICT-related incidents?

Financial entities must establish procedures and processes for identifying, handling and reporting ICT-related incidents as early as possible. Serious ICT-related incidents 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. Significant cyber threats must also be documented by financial entities, although reporting in this regard may be voluntary.

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 so-called TLPT tests at least in a 3-year cycle.

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

In order to effectively manage the ICT third-party risk, financial entities must, according to Art. 28 para. 3 DORA, keep an up-to-date information register relating to all contractual agreements on the use of ICT services provided by ICT third-party service providers. Before entering into a contractual agreement with an ICT third-party service provider, financial entities must also conduct a risk analysis with regard to the ICT third-party service provider on the basis of the criteria set out in Art. 28 para. 4 and para. 5 DORA. With regard to contract negotiations with ICT third-party service providers, financial entities must 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.

9. **How and by whom are ICT third-party service providers supervised under the DORA?**
The European supervisory authorities EBA, ESMA and EIOPA (so-called "ESAs") review ICT third-party service providers on the basis of specific criteria specified in Art. 31 para. 2 DORA and classify them as "critical" if necessary. 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?**
In order to enforce its powers under Art. 35 para. 1 lit. (a)-(c) DORA, the Lead Overseer may impose an administrative penalty payment 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 on a daily basis until compliance is achieved, but for no longer than six months. Penalty payments imposed are generally published by the Lead Overseer. With regard to 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 the 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, 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 tests are also specified and tightened by requiring extended tests based on TLPT. 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 has to be implemented into national law by 27 October 2024, DORA is to be considered lex specialis according to its recital 16.

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, TLPTs 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).

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

Financial entities and ICT third-party service providers should already start a GAP analysis now and close the identified gaps as soon as possible, at the latest by January 2025. Due to the extensive congruence with the already existing national and European provisions for the finance and insurance sector, an orientation towards these is appropriate for the implementation of the DORA. As additional guidance, the ESA will, in accordance with its obligation under Art. 28 para. 10 DORA, submit to the EU-Commission specifications regarding certain topics until 17 January 2024 by way of regulatory technical standards (RTS) and implementing technical standards (ITS). Four of these specifications have already been published on 19 June 2023 for public consultation until 11 September 2023 (available here). Additional publications of specifications for public consultation are expected until beginning of December 2023.

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
Senior Associate, Hamburg
IP/IT/Data Protection

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