ORACLE

Oracle Contract Checklist for the EU Digital Operational Resilience Act (DORA)

April 2023

Disclaimer

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their use of Oracle services. Please also note that the relevant contract(s) between you and Oracle determine(s) the scope of services provided and the related legal terms and this document is provided for reference purposes only, and is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and Oracle. Oracle disclaims any terms or statements contained herein that seek to impose legal or operational requirements on Oracle for the delivery of the services. Customers acknowledge that they remain solely responsible for meeting their legal and regulatory requirements.

The information in this document was current as of April 2023

Overview

Oracle has developed this document to help financial services customers operating in the European Union (**EU**) assess the use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications[1] in the context of the Digital Operational Resilience Act[2] (**DORA**). We want to make it easier for you as a financial entity to identify the sections of the Oracle Cloud services contract that may help you address your requirements.

In this document, you will find a list of requirements under DORA, along with references to the relevant sections of the Oracle Cloud services contract and a short explanation to help you conduct your review of the Oracle Cloud services.

The Oracle Cloud services contract includes the following customer-specific components, all of which are referenced in this document:

- **Oracle Cloud services agreement** – the Oracle Cloud Services Agreement (**CSA**) or Oracle Master Agreement (**OMA**) with Schedule C (Cloud)
- **FSA** – the Oracle Financial Services Addendum to the CSA or OMA, as applicable
- **Ordering Document** – Oracle Cloud services order
- **Services Specifications** – Service-specific components, including the **Oracle Cloud Hosting and Delivery Policies** with applicable **Services Pillar Document(s)** (Oracle SaaS Public Services Pillar Document, Oracle PaaS and IaaS Public Cloud Services Pillar Document, and Oracle Global Business Unit (GBU) Cloud Services Pillar Document, as applicable) and the **Oracle Data Processing Agreement** (**DPA**).

Regulatory Background

DORA forms part of the digital finance strategy adopted by the European Commission in 2020. It aims to establish a harmonised regulatory framework on digital operational resilience for financial entities operating in the EU. Its objectives include ensuring that financial entities can withstand, respond to and recover from information and communication technology (ICT)-related disruptions and threats, such as cyber threats. DORA applies to all authorised financial entities operating in the EU, subject to limited exceptions. It also creates an oversight framework for ICT third-party service providers to the financial sector that are deemed critical.

As a regulation, DORA is legally binding in all EU member states. It entered into force on 16 January 2023 and its provisions apply from 17 January 2025 following a 24-month implementation period. In the meantime, the European Supervisory Authorities will publish a series of regulatory technical standards (RTS) and implementation technical standards (ITS) to define requirements under DORA more concretely.

For information on other financial services regulations and guidelines, including the EBA Guidelines on outsourcing arrangements, please visit https://www.oracle.com/corporate/cloud-compliance/.

---

[1] Oracle Advertising SaaS services and NetSuite services are not included in the scope of this document.

[2] Regulation of the European Parliament and of the 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 Article 30 – Key contractual provisions

NO.	REQUIREMENT REFERENCE	DESCRIPTION	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	ORACLE EXPLANATION
Form of contract				
1.	Article 30(1)	The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document available to the parties on paper, or in a document with another downloadable, durable and accessible format.	Oracle Cloud services contract Cloud Hosting and Delivery Policies Cloud Services Pillar documentation Cloud Services Service Descriptions	The respective rights and obligations of the parties are set out in writing in the Oracle Cloud services contract. A customer's full services contract is available as a single electronic file upon request. Service level agreements are set out in the Cloud Hosting and Delivery Policies and associated Cloud Services Pillar documentation. Specifically, Section 3 of the Cloud Hosting and Delivery Policies, which form part of the services contract, references the target service availability level for cloud services, with exceptions, and any additional service level objectives, as applicable, specified in the relevant Cloud Service Pillar documentation or Service Descriptions.
Services and service levels				
2.	Article 30(2)(a)	The contractual arrangements on the use of ICT services shall include a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider.	Ordering Document Cloud Services Service Descriptions	The contracted services are described in the Ordering Document and in the relevant Cloud Services Service Descriptions.
3.	Article 30(2)(e)	The contractual arrangements on the use of ICT services shall include service level descriptions, including updates and revisions thereof.	Cloud Hosting and Delivery Policies Cloud Services Pillar documentation Cloud Services Service Descriptions.	Service level agreements are set out in the Cloud Hosting and Delivery Policies and associated Cloud Services Pillar documentation. Specifically, Section 3 of the Cloud Hosting and Delivery Policies, which forms part of the services contract, references the target service availability level for cloud services, with exceptions, and any additional service level objectives, as applicable, specified in the relevant Cloud Service Pillar documentation or Service Descriptions.
4.	Article 30(3)(a)	The contractual arrangements on the use of ICT services supporting critical or important functions shall include full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow an effective monitoring by the	Cloud Hosting and Delivery Policies Section 3 Cloud Services Pillar documentation	Section 3 of the Cloud Hosting and Delivery Policies references the target service availability level for cloud service as specified in the relevant Cloud Service Pillar documentation and Oracle's process for monitoring, measuring and reporting availability metrics to customers via the customer notifications portal. Customers can monitor the availability of Oracle cloud services by visiting the following sites:

		financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met.		○ Oracle Cloud Infrastructure: https://ocistatus.oraclecloud.com/ ○ Oracle Cloud Applications: https://saasstatus.oracle.com/ Information on monitoring the availability of certain other Oracle Cloud Application services is available upon request.
Monitoring and notification				
5.	Article 30(3)(b)	The contractual arrangements for the provision of critical or important functions shall include notice periods and reporting obligations of the ICT third-party service provider 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.	FSA Sections 7 and 6.2.2 Cloud Hosting and Delivery Policies Sections 1.12, 3.2.2, 4.1 and 5.2.1 DPA Sections 4.3, 5.3 and 9.2	Section 7 of the FSA states that Oracle provides support for cloud services through a cloud customer support portal. Service notifications and alerts relevant to cloud services are posted on this portal and include notification of circumstances that can reasonably be expected to have a material impact on the provision of the services. Oracle has other reporting and notification obligations, which are set out in the Cloud Hosting and Delivery Policies (Sections 1.12, 3.2.2, 4.1 and 5.2.1), the FSA (Section 6.2.2) and the DPA (Sections 4.3, 5.3 and 9.2). Additionally, as a listed company Oracle is subject to standard disclosure obligations on matters relevant to the public market.
Termination				
6.	Article 28(7)	Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances: • significant breaches by the ICT third-party service provider of applicable laws, regulations or contractual terms; • circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider; • ICT third-party service provider's evidenced weaknesses pertaining to the overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and confidentiality of data, whether personal or	CSA Section 9.4 OMA Schedule C Section 9.3 FSA Section 3.1	Section 9.4 of the CSA or Section 9.3 of the OMA Schedule C (as applicable) gives a customer the right to terminate if Oracle breaches a material term of the service contract and fails to correct the breach within 30 days. Section 3.1 of the FSA gives a customer the right to terminate cloud services on 30 days' written notice if: ○ there are weaknesses regarding the management and security of the customer's content or confidential information, ○ such termination is based on express instructions from the customer's financial services regulator, ○ Oracle is in breach of applicable law or regulation in providing the relevant cloud services, ○ impediments affecting Oracle's ability to perform the cloud services are identified, or ○ there are material changes affecting the cloud services or Oracle which result in an adverse impact of the provision of the cloud services.

		otherwise sensitive data, or non-personal data; • where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.		
7.	Article 30(2)(h)	The contractual arrangements on the use of ICT services shall include 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.	CSA Section 9.4 OMA Schedule C Section 9.3 FSA Section 3	The notice periods applicable to termination of the services are set out in Section 9.4 of the CSA or Section 9.3 of the OMA Schedule C (as applicable) and in Section 3 of the FSA.
8.	Article 30(3)(f)	The contractual arrangements for the provision of critical or important functions shall include 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.	FSA Sections 4.2 and 4.3	Section 4.2 of the FSA states that Oracle will, upon written request, continue to make services under the contract available for up to an additional 12 months from termination subject to certain conditions. Section 4.3 of the FSA explains that if a customer requires assistance with a transition, Oracle will enter into good faith negotiations regarding the provision of transition assistance services.

Subcontracting				
9.	Article 30(2)(a)	The contractual arrangements on the use of ICT services shall indicate whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such subcontracting.	FSA Section 6.1 DPA Sections 5 and 7.2 CSA Section 17.2 OMA Schedule C Section 14.2	Section 6.1 of the FSA contains a general written authorisation for Oracle to engage subcontractors that may assist in the performance of the services. If Oracle subcontracts any of its obligations under the services contract: ○ it will enter into a written agreement with the subcontractor reflecting, to the extent required based on the specific role of the subcontractor, obligations that are consistent with Oracle's obligations under the relevant terms of the services agreement ○ any such subcontracting will not diminish Oracle's responsibility towards the customer under the Services Agreement, and ○ Oracle will provide appropriate governance and oversight of the subcontractor's performance. Section 5 of the DPA contains a general written authorisation for Oracle to engage Oracle affiliates and third party subprocessors as necessary to assist in the performance of the services. That same section also confirms that those entities will be subject to the same level of data protection and security as Oracle under the terms of the services agreement and Oracle remains responsible for the performance of their obligations in compliance with the DPA and applicable data protection law. Section 7.2 of the DPA confirms that third party subprocessors are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information. Also refer to Section 17.2 of the CSA or Section 14.2 of the OMA Schedule C (as applicable).
Audit, access and information				
10.	Article 30(3)(e)	The contractual arrangements for the provision of critical or important functions shall include the right to monitor on an ongoing basis the ICT third-party service provider's 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	FSA Sections 1 and 2	Section 1 of the FSA grants customers and their third-party auditors access to relevant business premises and data used for providing the cloud services, as well as rights of inspection and auditing related to the cloud services, in each case as specified in the FSA. It also sets out Oracle's commitment to cooperate and provide reasonable assistance in relation to a customer audit Section 2 of the FSA grants the same audit and access rights to customers' financial services regulators and sets out Oracle's commitment to cooperate and provide reasonable assistance and information to such regulators in relation to their audits. Section 1.6 of the FSA states that if a customer is required by applicable law to take copies of relevant documentation during an on-site audit, Oracle will provide such copies provided that doing so does not threaten the security or integrity of Oracle networks or systems or other Oracle customers' data.

		by other contractual arrangements or implementation policies; • the right to agree alternative assurance levels if other clients' rights are affected; • the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections performed by the competent authorities, the lead overseer, financial entity or an appointed third party; • the obligation to provide details on the scope and procedures to be followed and frequency of such inspections and audits.		Section 1.5 of the FSA states that if the exercise of a customer's audit rights creates a threat or risk to Oracle networks or systems or other Oracle customers' service environments so that an audit request or right of access is denied, Oracle will use commercially reasonable efforts to provide an alternative way to deliver a similar level of assurance regarding the topic of the audit request or right of access that does not create such a threat or risk. Section 1.3 of the FSA explains that the audit plan for a requested audit will describe the proposed scope, duration, and start date of the audit. Other procedures applicable to audits are set out in Sections 1 and 2 of the FSA.
Location				
11.	Article 30(2)(b)	The contractual arrangements on the use of ICT services shall include the 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 if it envisages changing such locations.	Ordering Document Cloud Hosting and Delivery Policies Overview and Section 4.1.3	The Ordering Document or cloud customer support portal sets out the data center region applicable to the ordered Cloud services. The overview of the Cloud Hosting and Delivery Policies confirms that a customer's content will be stored in the data center region applicable to the services and that Oracle may replicate customer content to other locations within the applicable data center region in support of data redundancy. Section 4.1.3 of the Cloud Hosting and Delivery Policies states that Oracle may migrate services deployed in data centers retained by Oracle between production data centers in the same data center region as deemed necessary by Oracle or in the case of disaster recovery. For data center migrations for purposes other than disaster recovery, Oracle will provide a minimum of 30 days' notice to the customer. The locations of Oracle affiliates that may process personal information in connection with ordered cloud services are set out in the following list: https://www.oracle.com/corporate/oracle-affiliates.html The locations of Oracle's strategic sub-contractors and third-party sub-processors are available upon request.
Data and security				
12.	Article 30(2)(c)	The contractual arrangements on the use of ICT services shall include provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data.	DPA Sections 7 and 9 OMA Schedule C Sections 4 and 5 CSA Sections 4 and 5	The Oracle Cloud services contract addresses the availability, integrity, and confidentiality of customer content as follows: • Technical and organisational security measures: ○ Section 7 (Security and Confidentiality) of the DPA

			Cloud Hosting and Delivery Policies Sections 1, 3.1 and 3.2 SaaS Public Cloud Services Pillar Document PaaS and IaaS Public Cloud Services Pillar Document Oracle Global Business Unit Cloud Services Pillar Document	○ Section 1 (Oracle Cloud Security Policy) of the Cloud Hosting and Delivery Policies: ○ Relevant Pillar documentation ○ A summary of Oracle's Corporate Security Practices is set out in the following document: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf • Confidentiality and protection of customer content: ○ Section 4 of the CSA or Section 4 of the OMA Schedule C (as applicable) – specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) ○ Section 5 of the CSA or Section 5 of the OMA Schedule C (as applicable) ○ Section 9 (Incident Management and Breach Notification) of the DPA • Service Availability and Service Level Agreements: ○ Sections 3.1 and 3.2 of the Cloud Hosting and Delivery Policies ○ Relevant Pillar documentation
13.	Article 30(2)(d)	The contractual arrangements on the use of ICT services shall include provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the case of termination of the contractual arrangements.	CSA Section 9.5 Cloud Hosting and Delivery Policies Section 6.1 FSA Section 4.1 DPA Section 10.1	Section 9.5 of the CSA or Section 9.4 of the OMA Schedule C (as applicable) states that at the end of the services period, Oracle will make customer content available for retrieval by the customer during a retrieval period. Section 6.1 of the Cloud Hosting and Delivery Policies states that for a period of 60 days following termination of the services contract, Oracle will make available, via secure protocols and in a structured, machine-readable format, customer content residing in the production environment, or keep the service system accessible, for the purpose of data retrieval by customers. Section 4.1 of the FSA states that Oracle will provide reasonable assistance during the retrieval period to enable a customer to retrieve its content from the production environment, including assistance with understanding the structure and format of the export file. Any additional assistance may be agreed between the parties under a separate order. Section 10.1 of the DPA states that upon termination of the services, Oracle will promptly return, including by providing available data retrieval functionality, or delete any remaining copies of personal information on Oracle systems or services environments, except as otherwise stated in the services contract.

14.	Article 30(3)(d)	The contractual arrangements for the provision of critical or important functions shall include the obligation of the ICT-third party service provider to participate and fully cooperate in the financial entity's threat led penetration testing.	Cloud Hosting and Delivery Policies Section 3.4.2	Section 3.4.2 of the Cloud Hosting and Delivery Policies allows customers to conduct certain functional testing for Oracle cloud services in their test environments. Oracle conducts penetration tests of the Oracle OCI and SaaS systems annually. Oracle uses a commercial vulnerability scanning tool to scan external IP addresses and internal nodes monthly. Identified exploitable threats and vulnerabilities are investigated and tracked. In addition, Oracle completes third-party vulnerability scans/penetration tests annually for applicable services. The summary reports for third-party penetration tests are available upon request for entities that have signed a non-disclosure agreement with Oracle. In addition, customers are allowed to conduct penetration test of Oracle OCI cloud services as specified in the Oracle Cloud Security Testing Policies.
Business continuity and operational resilience				
15.	Article 30(3)(c)	The contractual arrangements for the provision of critical or important functions shall include requirements for the ICT third-party service provider 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.	FSA Section 5.1 Cloud Hosting and Delivery Policies Sections 1 and 2	Section 5.1 of the FSA confirms that Oracle will maintain a business continuity program with the objective of maintaining Oracle's internal operations used in the provision of cloud services and will monitor, test, and review the implementation and adequacy of the program annually. Section 2 of the Cloud Hosting and Delivery Policies describes Oracle's service continuity strategy and data back-up strategy. Section 1 of the Cloud Hosting and Delivery Policies describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption and training.
16.	Article 30(2)(f)	The contractual arrangements on the use of ICT services shall include the obligation of the ICT third-party service provider 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.	Cloud Hosting and Delivery Policies Section 5 DPA Section 9	Section 5 of the Cloud Hosting and Delivery Policies describes the support that Oracle provides to a customer in relation to ordered cloud services at no additional cost, which includes support in responding to ICT incidents. Section 9 of the DPA reflects Oracle's commitment to notify customers of a security breach involving customer content transmitted, stored or otherwise processed on Oracle systems or the cloud services environments and confirms that Oracle will take reasonable measures designed to identify the root cause(s).
17.	Article 30(2)(h)	The contractual arrangements on the use of ICT services shall include the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programs and digital operational resilience trainings.	FSA Section 5.2	Section 5.2 of the FSA states that in respect of any ICT security awareness programmes or digital operational resilience training a customer is required by applicable law and regulation to deliver to its staff or management, Oracle will participate by providing Oracle subject matter expertise for inclusion in the related programme or training materials, subject to additional fees at Oracle's then-current rates and as agreed in a professional services order executed by the parties.