

# Oracle Contract Checklist for Norwegian Financial Services Regulations Applicable to IT Outsourcing

- Regulations On The Use Of Information And Communication Technology (ICT) (FOR-2003-05-21-630)
- Financial Supervision Act (LOV-1956-12-07-1) and the Regulations on the duty to notify when outsourcing activities, etc (FOR-2021-09-15-2777)
- Circular 7/2021 (Guidelines on Outsourcing)

### **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 January 2024.

#### **Overview**

Oracle has developed this document to help financial services customers in Norway review Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications<sup>1</sup> in the context of the Regulations On The Use Of Information And Communication Technology (ICT), the Financial Supervision Act and the Regulations on the duty to notify when outsourcing activities, etc, and the Circular 7/2021 (Guidelines on Outsourcing). We want to make it easier for you as a financial services institution to identify the sections of the Oracle Cloud services contract that may help you address the requirements in these regulations. In this document, you will find a list of specific requirements under those regulations, along with a reference to the relevant section(s) 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 an Oracle Cloud Services Agreement (CSA) or Oracle Master Agreement (OMA) with Schedule C (Cloud)
- FSA The Oracle Financial Services Addendum to the Oracle Cloud Services Agreement (CSA) or Master Agreement (OMA) with Schedule C (Cloud)
- 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 Data Processing Agreement

## **Regulation Background**

This document will focus on the following regulations and guidelines introduced by the Financial Supervisory Authority of Norway ("Finanstilsynet", and previously known as "Kredittilsynet"):

- A. The <u>Regulations on the Use of Information and Communication Technology (ICT)</u> (the "Regulations") came into force on 1 August 2003 and were last amended in March 2022. They apply to Norwegian banks, insurance companies, pension funds, stock exchanges, investment firms etc. and lay down requirements applicable to ICT systems that are significant to an institution's business.
- B. The <u>Financial Supervision Act of 7 December 1956 No. 1</u>, which was last amended 15 June 2023, (the "Act") provides for the supervision of banks, mortgage companies, finance companies, payment institutions and account information service providers, electronic money institutions, etc., as well as corresponding foreign undertakings, to ensure that these institutions operate in an appropriate and proper manner in accordance with applicable law and attend to consumers' interests and rights. The <u>Regulations on the duty to notify when outsourcing activities, etc.</u>, which were issued under the Act and came into force in January 2022, elaborate on an institution's duty under the Act to notify Finanstilsynet of outsourcing agreements.



<sup>&</sup>lt;sup>1</sup> This checklist does not cover Industry Applications and NetSuite services.

C. The <u>Guidelines on Outsourcing</u> (the "Guidelines") were introduced by Finanstilsynet on 10 February 2020 and updated in December 2021. They apply to most financial service companies under the supervision of Finanstilsynet that have entered into an outsourcing agreement. Agreements for the provision of cloud services are typically considered outsourcing under the Guidelines.

Note the terms "Finanstilsynet", "Financial Supervisory Authority" and "regulator" are used interchangeably in this document. Please also note that the information below is based on unofficial English translations of the relevant Norwegian regulations.

For information on financial services regulations in other jurisdictions please visit <a href="https://www.oracle.com/corporate/cloud-compliance/">https://www.oracle.com/corporate/cloud-compliance/</a>

NO.	REGULATION REFERENCE	REGULATION REQUIREMENT/DESCRIPTION	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	ORACLE EXPLANATION
Due diligen	ce on the cloud services p	provider		
1.	Guidelines, section 5, Assessment of contractor	Before any outsourcing, the company must assess the contractor, as well as subcontractor(s) where this is relevant. The following conditions may be significant:	N/A	The responses provided in this section are in relation to pre-sales due diligence from a financial services customer on Oracle.
		a) Does the contractor have the necessary authorization where required?		a) Oracle does not require authorisation to provide cloud services to banking customers in Norway.  Section 17.5 of the CSA or section 14.3 of the OMA Schedule C, states that prior to signing an order for services, customer is solely responsible for determining whether the services meet its technical, business or regulatory requirements. Customer's responsibilities include obtaining approvals from its management and board of directors where required.
		b) Is there a relationship between the contractor and the company that can cause conflicts of interest?		b) and h): Oracle views ethical business conduct as a top priority and has implemented code of conduct policies along with a robust training program to train its employees and contractors on the highest ethical standards during their business dealings. See Oracle values and ethics policies and standards at oracle.com/corporate/citizenship/values-ethics.html#equal. The Oracle Code of Ethics and Business Conduct includes a chapter relating to conflicts of interests and redirecting to our Conflict of Interest Policy (Oracle internal document). The purpose of this policy is to help our employees identify and deal with situations that may give rise to potential conflicts of interest or the appearance of conflicts. The policy further details



c) Does the contractor have sufficient capacity, expertise and experience to perform the tasks in a responsible manner within the legislation that applies to the contractor? This also applies to tasks that the company, in its own emergency response plans, has assumed will be handled by the contractor and tasks that must be performed by the contractor if crisis solutions must be implemented.

d) Has the contractor established a

 d) Has the contractor established a satisfactory system for risk management and internal control?

e) Is the contractor certified, and if so, which controls form the basis of the current certification?

f) Does the contractor have sufficient financial strength to handle problems that may arise in the contractor's operations?

g) Where is the contractor located, and where will the tasks be performed? the processes for disclosures and approvals required where a potential or actual conflict of interest exists or if an employee is unsure whether one exists. As per the policy, employees must refrain from activities affected by the actual or potential conflict of interests while reviews are carried out. Customers remain responsible for carrying out their own due diligence within their organisation.

c); f) and h): Oracle (then Software Development Laboratories) has been trading since 1977. It went public in 1986. Today, it serves 430,000 customers in 175 countries and published a total GAAP revenue for the fiscal year 2021 of US\$40B.

Customer testimonies are available at https://www.oracle.com/customers/.

Annual reports and other corporate documentation may also be found at <a href="https://www.oracle.com/corporate/">https://www.oracle.com/corporate/</a>.

Please see notes in d) below and in the "Business continuity, incident management, system availability and testing" section with regards to emergency response plans.

d) Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as used in the Oracle Risk Management Resiliency Program (RMRP). Upon request by a customer, Oracle provides a summary of the RMRP, material modifications to the RMRP within the last 12 months, and pertinent program governance areas, along with confirmation that testing of these governance areas was performed within the last 12 months.

For additional information, visit.

e) Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations." These attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud services.

Details of Oracle's current certifications are available on the <u>Cloud Compliance</u> website, under the "Attestations" tab.

f) See the response for item c)

g) Cloud contracting with Norwegian customers typically goes through Oracle Norge AS, which is a Norwegian company registered and headquartered in Norway. Exceptions may apply to certain lines of business. The Oracle cloud services agreement



Among other things, this may be significant for:

- the risk of misuse or loss of personal data and other confidential information
- which legislation and which control and law enforcement regimens apply to the contractor and the contractor's activities
- the ability of the company and the Financial Supervisory Authority to perform physical checks.
- h) Does the contractor have a good reputation?
- Does the contractor follow principles for good corporate governance and does the contractor act in a manner that is consistent with the company's values and ethical guidelines? Assessment criteria may, for example, be the contractor's relationship to international standards for human rights and the UN's sustainability goals, such as working conditions, environmental protection, etc.

specifies the law applicable to such agreement, which is usually Norwegian law for Norwegian customers contracting with Oracle Norge AS.

For the performance of cloud services, Oracle uses a "follow the sun" model, whereby tasks may be performed by resources in Oracle affiliates and subcontractors all over the world. Lists of the Oracle affiliates, subprocessors and strategic subcontractors, with their respective location, engaged in the delivery of cloud services are available via My Oracle Support. In relation to the handling of confidential information, including personal data, please see notes in the "Data processing and Confidentiality" section below. Please see notes in the section "Audit rights for regulators" below regarding the ability of the Financial Supervisory Authority to perform physical checks. Regarding law enforcement requests by e.g. public and government authorities, please see section 11 of the DPA "Legal Requirements" and the information at <a href="https://www.oracle.com/legal/law-enforcement-requests-report/">https://www.oracle.com/legal/law-enforcement-requests-report/</a>

- h) See the responses for items b) and c)
- k) Oracle is committed to maintaining high standards of business ethics and complying with applicable laws. Accordingly, we draw your attention to the following:
- 1. Oracle has implemented the <u>Oracle Code of Ethics and Business Conduct</u> ("Code") and adopted formal processes for enforcing compliance with the Code. In addition, Oracle has implemented an Anti-Corruption Policy that addresses in more detail Oracle's anti-corruption and maintenance of books and records requirements and business courtesy guidelines. All Oracle employees are subject to the Code and to the Anti-Corruption Policy and are required to take on-line ethics training upon hire and biannually thereafter. Oracle also maintains a robust training program for all employees to drive their understanding of, and compliance with, anti-corruption laws.
- 2. Oracle has implemented the <u>Oracle Partner Code of Conduct and Business Ethics</u> that applies to members of the Oracle Partner Network ("OPN"), including distributors and resellers and their personnel throughout the world. OPN members are contractually required to comply with the terms of the Oracle Partner Code of Conduct and Business Ethics. Those that distribute to public sector entities are subject to additional contractual requirements intended to ensure their compliance with anti-corruption laws. In addition, those that distribute to public sector entities in the areas of the world considered high-risk to Oracle are subject to due diligence.
- 3. Oracle has implemented the <u>Oracle Supplier Code of Ethics and Business Conduct</u> that applies to Oracle suppliers and service providers and their personnel throughout the world. Oracle suppliers and service providers are contractually required to comply with the terms of the Oracle Supplier Code of Ethics and Business Conduct.



The outsource	cing agreement			4. Oracle has implemented corporate governance practices and sustainable business practices. Oracle is committed to good citizenship and fostering a culture of corporate social responsibility. We are also committed to integrating respect for human rights into our global operations and value chain. Our long-standing commitment to uphold and respect human rights for all people, is reflected in Oracle's Code of Ethics and Business Conduct, and in our policies, practices and core values. Human rights span a broad array of fundamental rights, freedoms and standards of treatment of all people adhered to by governments, businesses and individuals as described in the United Nations Universal Declaration of Human Rights, the ILO Declaration on Fundamental Principles and Rights at Work, the UN Global Compact, the UN Guiding Principles on Business and Human Rights and relevant laws and regulations. Furthermore, Oracle does not tolerate or condone human trafficking or slavery in any part of its global organization and requires that contractors, subcontractors, vendors, suppliers, partners and others through whom Oracle conducts business not engage in any practice that constitutes trafficking in persons or slavery.  Oracle's annual proxy filing contains a further description of the company's compliance and ethics program: <a href="http://investor.oracle.com/financial-reporting/proxy-and-electronic-delivery/default.aspx">http://investor.oracle.com/financial-reporting/proxy-and-electronic-delivery/default.aspx</a> : Information about Oracle's corporate governance practices can be found at: <a href="https://www.oracle.com/corporate/corporate-governance.html">https://www.oracle.com/corporate/corporate-governance.html</a> : You can find more on Oracle Corporate Citizenship at <a href="https://www.oracle.com/corporate/corporate/citizenship/">https://www.oracle.com/corporate/corporate/citizenship/</a>
2.	Regulations, Section 12, Outsourcing	The supplier shall be contractually committed to supplying services that are consistently compliant with the ICT regulations.	<ul><li>Oracle Cloud services agreement</li><li>Ordering Document</li><li>FSA</li></ul>	An Oracle Cloud services agreement (and an Ordering Document must be signed before Oracle starts providing Cloud services. The Financial Services Addendum (FSA) may be appended to the Oracle Cloud services agreement to address regulatory requirements not already covered in the Oracle Cloud services agreement and Oracle policies' applicable to the Cloud services.
3.	Guidelines, section 6, The Outsourcing Agreement  The agreement on outsourcing shall be in writing and contain at least:	The agreement on outsourcing shall be in writing and contain at least:	• Services Specifications	
		contracting parties (business	<ul><li>Oracle Cloud services agreement</li><li>Ordering Document</li></ul>	Contracting parties are identified by name in the Oracle Cloud services agreement and in the Ordering Document.
		<ul> <li>b) Clear description of what the assignment is based on, including specification of the delivery with quality goals</li> </ul>	<ul><li>Ordering Document</li><li>Services Specifications</li></ul>	The description of the ordered services can be found in the Ordering Document and in the Services Specifications/Services Description for those services.

c) Agreement term and notice period	<ul> <li>CSA, section 9 or OMA General Terms, sections 2 and 6 with Schedule C, section 9</li> <li>Ordering Document</li> </ul>	The agreement term and termination provisions (including related notice periods) can be found in the Oracle Cloud services agreement. The duration of ordered cloud services ("Services Period") is stated in the relevant Ordering Document.
d) Special right for the company to terminate the agreement	<ul> <li>CSA, section 9 or OMA Schedule C, section 9</li> <li>FSA, section 3</li> </ul>	A customer's termination rights are set out in section 9 of the CSA or section 9 of the OMA Schedule C, as applicable, and in section 3 of the FSA.
e) The company's right to monitor the execution of the task(s)	<ul><li>FSA, sections 1 and 7</li><li>DPA, section 8</li></ul>	Customers can monitor the ordered services, and Oracle's compliance with the agreement, by exercising their audit rights under section 1 of the FSA and section 8 of the DPA.
f) The right of the company to require information or reporting in the format necessary for the company to be able to monitor outsourced activities and to be able to fulfil the company's own reporting obligations		Additionally, customers can monitor the availability of Oracle Cloud services by visiting the following sites <sup>2</sup> :  • Oracle Cloud Infrastructure: <a href="https://ocistatus.oraclecloud.com/">https://ocistatus.oraclecloud.com/</a> • Fusion Cloud Applications: <a href="https://saasstatus.oracle.com/">https://saasstatus.oracle.com/</a> The Oracle Cloud services agreement sets out the notifications that customers are
g) A provision that ensures the company ongoing monitoring that the contractor is complying with the duty of confidentiality and that the company's obligations under personal data legislation are being fulfilled		entitled to receive, which may help enable them to monitor the outsourced services. In particular, section 7 of the FSA states that Oracle provides support for the Oracle 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, the FSA and the DPA.
h) The right of the Financial Supervisory Authority to access all information deemed necessary as part of its supervision of the company, and to supervise outsourced activities without restrictions	• FSA, section 2	See section 2 of the FSA, which sets out the audit and access rights of customers' financial services regulators.



 $<sup>^2\,</sup> Information\, on\, monitoring\, the\, availability\, of\, certain\, other\, Oracle\, Cloud\, Application\, services\, is\, available\, upon\, request.$ 

<ul> <li>Bans on subcontracting, unless the contractor shall have such a right; see letters o) - r).</li> </ul>	<ul><li>FSA, section 6</li><li>DPA, section 5</li></ul>	Section 6.1 of the FSA and section 5.1 of the DPA together contain general written authorizations for Oracle to engage subcontractors, Oracle Affiliates and third party subprocessors to assist in the performance of the services.
In addition, the company must assess whether there is a need to regulate the following conditions:		
j) Special requirements for how the contractor is organized, soundness, ownership, insurance coverage, provision of guarantees, etc., and, in such a case, what shall apply if there are any changes in these prerequisites. For example, prior consent or a duty to notify the company with any deadlines for notification may be required.	Ordering Document	Oracle maintains various types and levels of insurance from highly rated insurance carriers covering its locations on a worldwide basis. Oracle generally takes out and maintains certain insurance coverages. Through insurance and/or operating cash, Oracle has the ability to pay the limits on liability set out in the Oracle Cloud services contracts. Oracle contracts may specify applicable insurance coverage and limits in the Ordering Document. Please also see the information in section 1 "Due diligence on the cloud services provider" above, paragraph c).
<ul> <li>k) Choice of law and where a dispute is to be decided (which country)</li> </ul>	CSA, section 14 or OMA General Terms, section 13	Choice of law and competent jurisdiction for disputes are stated in section 14 of the CSA or section 13 of the OMA General Terms, as applicable.
The contractor's duty to cooperate with relevant authorities in an emergency response situation when this is a requirement in the sector regulations	• FSA, section 2	Section 2 of the FSA details the audit and access rights of 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.
m) Clear description of the parties' obligations upon termination of the agreement, including the contractor's obligations to assist in the liquidation phase. For example, a duty for the contractor to contribute to securing and transferring data to the company or another recipient that the company determines, and in the format requested by the company	<ul> <li>CSA, section 9 or OMA Schedule C, section 9</li> <li>FSA, section 4</li> </ul>	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 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 by the parties.  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.

		n) That the contractor is obliged to handle the tasks that the company has assumed in determining its own emergency response plans, including the obligation for the contractor to contribute to the implementation of crisis solutions.	<ul> <li>FSA, section 5</li> <li>Oracle Cloud Hosting and Delivery Policies, section 2</li> </ul>	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.  n) Section 5 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.  Further information about the resilience framework that Oracle maintains for its operations can be found in the Oracle Risk Management Resiliency Program data sheet available at: https://www.oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf
Subcontracti	ing			
4.	Guidelines, section 6, The Outsourcing Agreement	Provisions on subcontracting by the contractor  If the contractor is to be entitled to outsource tasks to others (use subcontractors in one or more lines), this must be the result of an agreement between the company and the contractor. If so, the company must always:		
		<ul> <li>Assess whether restrictions shall be imposed on who may be a subcontractor(s), whether the company's consent shall be necessary, etc.</li> </ul>	<ul><li>FSA, section 6</li><li>DPA, section 5</li></ul>	<ul> <li>o) Section 6.1 of the FSA and section 5.1 of the DPA together contain general written authorizations for Oracle to engage subcontractors, Oracle Affiliates and third party subprocessors to assist in the performance of the services,</li> <li>Under section 6.2 of the FSA and section 5.4 of the DPA, a customer may object to the intended involvement of a strategic subcontractor or third-party subprocessor in the provision of the services and, if the matter cannot be resolved, the customer may terminate the relevant services.</li> </ul>
		<ul> <li>Ensure that both the company and the Financial Supervisory Authority have the same rights regarding</li> </ul>	• FSA, sections 1 and 2	p) Sections 1.1 and 2.1 of the FSA confirm that the audit and access rights granted to customers and financial services regulators under the FSA also apply in respect of Oracle's strategic subcontractors.



		subcontractors as regarding contractors		
		q) Clarify the contractor's responsibility to ensure that subcontractors comply with the duty of confidentiality and that the company's obligations pursuant to personal data legislation are fulfilled	<ul> <li>FSA, section 6</li> <li>DPA, sections 5 and 7</li> </ul>	q) As stated in section 6.1 of the FSA, 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, which includes non-disclosure and data security commitments.  Section 5.2 of the DPA confirms that any Oracle affiliates or third party subprocessors engaged to assist in the performance of the services 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 states 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.
		r) Ensure that one's own reporting obligation to the Financial Supervisory Authority can be complied with in situations where changes in the subcontracting situation are notifiable. Notification deadlines must be set so that the company can report on time to the Financial Supervisory Authority.	<ul><li>FSA, section 6</li><li>DPA, section 5</li></ul>	r) Section 6.2.2 of the FSA sets out a process by which customers may sign up to receive notification of any intended changes to Oracle's lists of strategic subcontractors, and section 5.3 of the DPA sets out a process by which customers may sign up to receive notification of any intended changes to Oracle's lists of Oracle affiliates and third party subprocessors.
Change man	agement			
5.	Regulations, Section 9, Problem and change management	The institution shall ensure that procedures are in place for the management of problems and changes, and that they are complied with.  The change management procedures shall cover all changes that may affect the ICT systems and shall ensure proper, formal treatment and documentation of the changes. The institution shall ensure that the change management procedures	<ul> <li>CSA, section 1.2 or OMA Schedule C, section 1.2</li> <li>FSA, section 7</li> <li>Oracle Cloud Hosting and Delivery Policies, section 4</li> </ul>	In section 1.2 of the Cloud Services Agreement, Oracle reserves the right to unilaterally "update the Services and Service Specifications (with the exception of the Data Processing Agreement []) to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of system use, and availability of Third Party Content [(as defined in the Cloud Services Agreement)]". However, section 1.2 also states that "Oracle updates to the Services or Service Specifications will not materially reduce the level of performance, functionality, security or availability of the Services during the Services Period of Your order.".  Customers may sign up to receive notice of updates to the Oracle Cloud Hosting and Delivery Policies and the DPA (and certain other Services Specifications made available by Oracle) at <a href="https://www.oracle.com/corporate/contracts/cloud-services">www.oracle.com/corporate/contracts/cloud-services</a> .

		provide stable, planned and predictable ICT operations.		The Oracle Cloud Change Management Policy in the Oracle Cloud Hosting and Delivery Policies describes notably maintenance activities for the services, data centre migrations and software updates.
Notification	requirements			
6.	Act, section 4c (notification requirements)	Undertakings as mentioned in section 1 shall notify Finanstilsynet when entering into an agreement on the outsourcing of services, and of any subsequent changes to such an agreement and any change of contractor. The notification shall be given at least 60 days prior to the entry into force of the agreement, changes to the agreement or change of contractor.	<ul><li>DPA, section 5</li><li>FSA, section 6</li></ul>	Section 5.3 of the DPA confirms that Oracle maintains lists of Oracle affiliates and third party subprocessors that may process personal information and sets out a process by which customers may sign up to receive notice of any intended changes to these lists.  Section 6.2.2 of the FSA confirms that Oracle maintains lists of its strategic subcontractors and sets out a process by which customers may sign up to receive notice of any intended changes to these lists.  Upon discussion with Oracle at contracting stage, Oracle may discuss with you the possibility of increasing the standard 30-day notice period under the DPA section 5.3 and the FSA section 6.2.2 to 90 days if you need to give 60 days' prior notice of changes
7.	Regulations on the duty to notify when outsourcing activities, etc., §3, Outsourcing agreements subject to notification	The duty to notify when outsourcing pursuant to section 4c of the Financial Supervision Act applies to agreements on outsourcing of activities that are critical or important to the company.		of subcontractors to your financial services regulator.
8.	Regulations on the duty to notify when outsourcing activities, etc., §4, Requirements for notification	Notification of outsourcing of business shall contain information about:  a. name and organization number of the contractor  b. the business / tasks that are outsourced	a), b), c), e): c.f. Oracle Cloud services contract; d): FSA, section 6, Subcontracting; f) FSA, section 1, Audit	The Oracle Cloud services contract will contain the information required in points a) through to c) and e). Lists of subcontractors are available on My Oracle Support, as described in row 8 above. In relation to point f), customers are able to monitor the agreement and the provision of the cloud services through the Services Notifications mechanism and by exercising their audit rights under the FSA.
9.	Guidelines, section 7.3, Further information on notifications under the Financial Supervision Act Section 4c and processing by the Financial Supervisory Authority; Content of notification	c. The contractor conducts business in Norway, in a Norwegian company, in a branch or as a cross-border business. If the contractor is established abroad, it must also be stated in which country the company's head office is established in d. names and organization numbers of subcontractors that the contractor uses when performing tasks on behalf of the company. If a subcontractor is established abroad, you are asked which country	and access rights for You, and section 7, Service Notifications	



Data process	sing and Confidentiality	e. the agreement's start-up and termination date, including information on the rolling agreement period  f. how the company will follow up its responsibility for the outsourced business, as well as the company's risk assessment of the outsourcing.  Notification of outsourcing of ICT activities shall also contain:  a. the outsourcing agreement with attachments  b. minutes of the board meeting where it is stated that the board has considered the outsourcing agreement and risk assessment of the outsourcing.		
10.	Regulations, Section 8, Operation	The operation of ICT processes shall be based on written procedures that ensure complete, timely and correct data processing and data storage.	<ul> <li>Oracle Cloud services agreement, section 6</li> <li>DPA</li> <li>Oracle Cloud Hosting and Delivery Policies, sections 1 and 3</li> <li>Oracle PaaS and laaS Public Cloud Services Pillar, sections 1 and 3</li> <li>Oracle SaaS Public Cloud Services Pillar, sections 1 and 3</li> <li>Oracle Corporate Security Practices</li> </ul>	The Oracle Cloud services agreement stipulates that Oracle warrant that during the Services Period we will perform the Services in all material respects as described in the Service Specifications, most notably the Oracle Cloud Hosting and Delivery Policies and the relevant Pillar document for the cloud services ordered. The DPA further describes how Oracle processes personal data when performing the cloud services.  The Oracle Cloud Hosting and Delivery Policies and the Pillar Documents provide further details on how a customer's content is processed and stored in accordance with the Oracle Cloud Security Policy and the Oracle Cloud Service Level Agreement Policy.  The Oracle Corporate Security Practices describe the measures taken by Oracle in respect of information security, operations management and resilience management to protect the security and integrity of the data hosted and processed by Oracle.
11.	Regulations, Section 12, Outsourcing	The agreement shall also provide for secure management of confidential information.	<ul><li>CSA, sections 4 and 5</li><li>DPA, section 7</li></ul>	Sections 4.3 and 5 of the CSA or sections 4 and 5 of Schedule C of the OMA, as applicable, outline the general obligations of Oracle in relation to protecting customer's confidential information.



12.	Guidelines, section 4.3, Information management	Statutory confidentiality or duties related to information management do not normally prevent the company from outsourcing tasks that involve the contractor obtaining access to such information. See more about this in the Financial Supervisory Authority's guide on confidentiality (Circular 3/2019). The company is obliged to implement risk mitigation measures that prevent loss and misuse of information, for example in the use of confidentiality statements. Special requirements for protecting information may follow from other regulations, such as requirements for a data processing agreement. The company's assessment of the contractor and the regulation and monitoring of information management in the agreement are important contributions in preventing information from getting lost, cf. Sections 5 and 6, respectively.	<ul> <li>Oracle Cloud Hosting and Delivery Policies, section 1</li> <li>Oracle Corporate Security Practices</li> <li>Oracle PaaS and laaS Public Cloud Services Pillar Document, section 1</li> <li>Oracle SaaS Public Cloud Services Pillar, Section 1</li> </ul>	Section 7 of the DPA states that Oracle has implemented and will maintain appropriate technical and organizational security measures for the processing of personal information.  Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy, which outlines Oracle's security practices. These practices are further detailed in the Oracle Corporate Security Practices.  Section 1 of the applicable Services Pillar Document also addresses security measures, including physical safeguards.
Audit rights	for customers			
13.	Regulations, Section 12, Outsourcing	The agreement must ensure that institutions under supervision are given the right to control and audit all activities carried out by the service provider under the agreement.	• FSA, section 1	Section 1 of the FSA grants a customer access to relevant business premises and rights of inspection and auditing related to the Cloud services to enable the customer to monitor the outsourcing arrangement and compliance with all applicable regulatory and contractual requirements.
Audit rights	for regulators			
14.	Regulations, Section 12, Outsourcing	The agreement shall further ensure that Finanstilsynet has access to information from the service provider and has a right to inspect the service provider if Finanstilsynet deems this to be necessary as part of its supervision of the institution.	• FSA, section 2	Section 2 of the FSA grants a customer's financial services regulator the same access to relevant business premises and rights of inspection and auditing related to the Cloud services as granted to the customer under section 1 of the FSA. Section 2.1 provides that a customer's regulator may audit Oracle as required by applicable law. Section 2.4 explicitly acknowledges the information-gathering and investigatory powers of resolution authorities.
15.	Guidelines, section 4, Limitation on the	Supervision of the outsourced activities by the Financial Supervisory Authority: the company must ensure that the Financial		Also refer to section 2.5 of the FSA, which states that Oracle will cooperate with a customer's financial services regulator and provide reasonable assistance in accordance with applicable law.



	tasks that can be	Supervisory Authority can supervise					
	outsourced	outsourced activities					
Business co	Business continuity, incident management, system availability and testing						
16.	Regulations, Section 8, Operation	ICT operational procedures shall be documented and shall ensure that ICT systems are available as specified in the institution's written requirements. To avoid disruption to the ICT systems or their surroundings that may have a negative impact on the fulfilment of the written requirements, regular analyses and measures shall be carried out.  The institution shall test and document that the ICT operation is in line with the written requirements laid down by the	<ul> <li>FSA, section 5</li> <li>Oracle Cloud Hosting and Delivery Policies, section 2</li> <li>Oracle PaaS and laaS Public Cloud Services Pillar Document, particularly section 2</li> <li>Oracle SaaS Public Cloud Services Pillar Document,</li> </ul>	Oracle's business continuity plans do not replace or supersede Customers' own business continuity plans and only relate to Oracle's operations.  Section 5 of the FSA confirms that Oracle maintains a business continuity program and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Upon at least 30 days' notice by you no more than once per calendar year, Oracle will make available to you via web conference or on Oracle premises, in a guided manner, a summary of the program and applicable test information, material modifications to the program within the last 12 months, and pertinent governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months.  Additionally, see the Oracle Cloud Service Continuity Policy in section 2 of the Oracle Cloud Hosting and Delivery Policies.			
		institution.	particularly section 2	Section 2 of the Pillar Documents also addresses cloud service continuity.			
17.	Regulations, section 11, Business disruptions and crisis management	The institution shall have a documented crisis management plan which shall be activated if ICT operations cannot be upheld due to a crisis. The term 'crisis' means [unintended] events which cause a disruption so that the institution is unable to maintain its ICT operations with its regular resources.  The crisis management plan must as a minimum include:  - an overview of ICT systems included in the plan  - a description of a fallback solution  - clear-cut criteria for activation of the fallback solution  - acceptable downtime in case of disruption of operations, before the fallback solution is activated  - procedures containing the actions necessary to restore ICT operations  - an overview of responsibilities and procedures upon activation of the fallback		Oracle deploys its cloud services on a resilient computing infrastructure designed to maintain service availability and continuity if an adverse event affects the services. Availability domains align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintains generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place.  To learn more about physical and environmental controls customers may consult the information available at <a href="https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html">https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html</a> .  Oracle's Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency frameworkto help facilitate an efficient response to business-interruption events affecting operations. Disaster recovery is a key subprogram of Oracle RMRP. Oracle's corporate Disaster Recovery (DR) plans focuses on the resiliency of computing infrastructure supporting Oracle's internal operations. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in			



		- directions for informing affected employees, suppliers, customers, public authorities and media.  Training, exercises and tests shall be conducted at least once a year to ensure that the crisis management plan and fallback solution function as intended. The results shall be documented.		in conjunction with other recovery strategies to both protect against disruption and enable recovery of services.  Crisis Management  Each critical Oracle line of business maintains a business continuity plan that includes a business impact analysis (BIA), risk assessments, and disaster recovery contingency plans. The plans align with Oracle's Risk Management and Resiliency Program policy, which requires the plans to outline procedures, ownership, roles, and responsibilities to be followed if a business disruption occurs. These plans are reviewed and tested annually.  Other available resources  Oracle provides various resources, such as compliance reports and guidance documents, through the Oracle Cloud Console and My Oracle Support that may assist customers in their dialogue with competent authorities. In addition, as required by applicable law or regulation, Oracle provides customers and their regulators with necessary information (including summaries of reports and documents) regarding the activities outsourced to Oracle.
18.	Regulations, Section 9, Problem and change management	The institution shall ensure that procedures are in place for the management of problems and changes, and that they are complied with.  The procedures for problem management shall cover all problems that arise in the operation of the ICT systems. The objective of problem management is to restore normal operational conditions for ICT activities. Problem management shall identify the cause of the problem as well as prevent its recurrence and shall ensure proper and formal treatment of the problem. The problems shall be documented. The procedures for problem management shall contain escalation guidelines.  Operational or security incidents causing a significant reduction in functionality as a result of breach of confidentiality (protection of data), integrity (protection against unauthorised changes) or availability of ICT systems and/or data	<ul> <li>FSA, section 7</li> <li>DPA, section 9</li> <li>Oracle Cloud Hosting and Delivery Policies, section 5</li> <li>Oracle Corporate Security Practices</li> </ul>	As stated in section 7 of the FSA, Oracle provides notifications and alerts relevant to cloud services via the cloud customer support portal, subject to customers signing up to receive such notifications and alerts. Those notifications and alerts include notification of circumstances that can reasonably be expected to have a material impact on the provision of cloud services.  Section 9 of the DPA addresses Oracle obligations in relation to incident management and breach notifications applicable to customer's personal data.  The Oracle Cloud Support Policy in the Oracle Cloud Hosting and Delivery Policies describes the support provided by Oracle to resolve issues with the services in accordance with that policy.  As set out in the Oracle Corporate Security Practices, Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been accessed by an unauthorized entity. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to such security events and incidents. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Oracle recommends post-incident analysis to identify opportunities for reasonable measures which improve security posture and defence in depth. In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the DPA.

		shall be reported to Finanstilsynet without undue delay. Reports should normally cover incidents which the institution itself categorises as very serious or critical, but may also cover other incidents that reveal particular vulnerabilities in applications, architecture, infrastructure or defences. Institutions listed in section 1, first subsection no. 12 (real estate agencies) are exempt from the incident reporting requirement.		Additionally, depending on the service infrastructure type and notification scenario (Outage, Maintenance, Informational, Action Required), Oracle provides several different communication channels used for customer notifications including through:  - OCI Status: https://ocistatus.oraclecloud.com/#/ - Oracle Cloud Console, and - My Oracle Support.
Termination				
19.	Act, section 4c (termination of the outsourcing agreement)	Finanstilsynet may set terms and conditions for the outsourcing or order the undertaking not to initiate or to terminate the assignment if Finanstilsynet finds that the outsourcing is of a scope or manner that cannot be considered to be appropriate, which complicates the supervision of the outsourced activities or the undertaking's total operations, or is in conflict with provisions laid down in or pursuant to law."	• FSA, section 3.1	A customer's termination rights under the FSA include the right to terminate the cloud services on 30 days' prior notice where the continued use of the services would cause customers to violate applicable law and regulation upon the conclusion made by the regulator and where termination is based on express instruction issued by the customer's financial services regulator.
20.	Guidelines, section 2, Assessments that must be conducted before outsourcing	Termination right for company:  The Company's assessment must also include the possibility of terminating the agreement without it causing significant disruption to the business, and in a manner that ensures compliance with legal requirements and obligations to customers. In connection with this, the following possibilities must be considered:  - the movement of outsourced functions and data to alternative providers;  - taking the task back into the company, including access to capacity and expertise;	<ul> <li>CSA, section 9</li> <li>OMA Schedule C, section 9 or CSA section 9, as applicable</li> <li>FSA, section 3</li> <li>FSA sections 4 and 11.3</li> <li>Oracle Cloud Hosting and Delivery Policies, section 6.1</li> <li>Oracle PaaS and laaS Public Cloud Services</li> </ul>	Under section 3 of the FSA, if at any time during the Services Period of the relevant ordering document the customer has a reason to believe that the continued use of the cloud services will put them in contravention of applicable law which might lead to action by their Financial Services Regulator, they must promptly notify Oracle so that the customer and Oracle can discuss options (such as amending the Oracle Cloud services contract) enabling the continued use of the cloud services. Customers have the right to terminate the cloud services in the following situations:  Termination due to regulatory requirements  Continued use of the services would cause customers to violate applicable law and regulation upon the conclusion made by the regulator.  Termination requested based on express instruction issued by the regulator where the services are considered as an impediment to effective supervision over the customer.  Termination due to insolvency  Oracle has become insolvent or resolved to go into liquidation.



		any other measures that ensure the continuous delivery of outsourced activities.  The company must ensure that there is a legal right to terminate the agreement.	Pillar Documentation, section 6  Oracle SaaS Public Cloud Services Pillar Documentation, section 6	<ul> <li>A proposal is made for entering into any compromise or arrangement with any or all of Oracle's creditors.</li> <li>A receiver is appointed over all or substantially all the assets of Oracle.</li> <li>Additionally, sections 6.1 and 9.4 of the CSA and sections 6.1 and 9.3 of Schedule C, as applicable, further explain that customers have the right to terminate for any breach of a material contract term, including a breach of the service warranty. In the service warranty, Oracle warrants that it will perform the services using commercially reasonable care and skill in all material respects as described in the Service Specifications.</li> <li>Pursuant to section 4 of the FSA, "Exit Provision," customers are able to order transition services and transition assistance to facilitate the transfer or the reincorporation of the concerned function back to the customer or to a third-party provider.</li> </ul>
21.	Guidelines, section 7.5, Powers of the Financial Supervisory Authority in the event of outsourcing	Pursuant to Section 4c, second paragraph, of the Financial Supervision Act, the Financial Supervision Act, the Financial Supervisory Authority may set conditions for outsourcing, order the company not to implement a contract for outsourcing or order termination of the assignment.  The sector regulations also give the Financial Supervisory Authority the authority to intervene in the case of outsourcing activities. For example, the Financial Supervisory Authority has the authority under the Financial Companies Act to terminate or change contracts concluded by a financial institution when necessary as part of crisis management. In such situations, the Financial Supervisory Authority also has the authority to order the financial company to hand over tasks to a contractor.		

## **Connect with us**

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.









Copyright © 2024, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC\_US@oracle.com.

