SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Oracle Corporation (Oracle Cloud Infrastructure)

Verification-ID	2022LVL02SCOPE4214
Date of Approval	August 2023
Valid until	August 2024

Table of Contents

1 Verification against v2.11 of the EU Cloud CoC 3

2 List of declared services 3

2.1 Oracle Cloud Infrastructure 3

3 Verification Process - Background 5

3.1 Approval of the Code and Accreditation of the Monitoring Body 5

3.2 Principles of the Verification Process 6

3.3 Multiple Safeguards of Compliance 6

3.4 Process in Detail 6

3.4.1 Levels of Compliance 7

3.4.2 Final decision on the applicable Level of Compliance 9

3.5 Transparency about adherence 9

4 Assessment of declared services by Oracle (see 2.) 9

4.1 Fact Finding 9

4.2 Selection of Controls for in-depth assessment 10

4.3 Examined Controls and related findings by the Monitoring Body 10

4.3.1 Examined Controls 10

4.3.2 Findings by the Monitoring Body 10

5 Conclusion 12

6 Validity 12

1 Verification against v2.11 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.11 (**'v2.11'**)[2] as of December 2020.

Originally drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers – was developed against Directive 95/46/EC[4] and incorporated feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code (v2.11) and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

2 List of declared services

2.1 Oracle Cloud Infrastructure[6]

Oracle Cloud Infrastructure is a set of complementary cloud services that enables customers to build and run a wide range of applications and services in a highly available hosted environment. Oracle Cloud Infrastructure offers high-performance compute capabilities (as physical hardware or virtual instances) and storage capacity in a flexible overlay virtual network that is securely accessible from customers' on-premise networks.[7]

The Oracle Cloud Infrastructure Service Family as in scope of this declaration of adherence consists of the following Cloud Services:

- Access Governance
- Account Tracking and Automation Tool
- Accounts Management
- Analytics Cloud
- Anomaly Detection
- API Gateway
- Application Dependency Management
- Application Performance Monitoring
- Archive Storage
- Artifact Registry
- Audit

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[6] https://www.oracle.com/cloud/
[7] **NOTE**: The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

- Autonomous Database on Cloud@Customer
- Autonomous Database on Dedicated Exadata Infrastructure
- Autonomous Database on Shared Exadata Infrastructure
- Bare Metal and Virtual Machine Database Systems
- Bastion
- Big Data
- Bling
- Block Volume
- Blockchain Platform
- Budgets
- Certificates
- Classic Migration
- Client Logging
- Cloud Advisor
- Cloud Guard
- Cloud Incident Service
- Cloud Shell
- Compute
- Console Announcements
- Container Engine for Kubernetes
- Container Instances
- Content Management
- Customer Feedback Service
- Data Catalog
- Data Flow
- Data Integration
- Data Labeling
- Data Safe
- Data Science
- Data Transfer
- Database Management
- Database Migration
- Database Tools
- DDoS Protection
- DevOps – Build Service
- DevOps – Deployment Pipelines
- DevOps – Project Service
- DevOps – Source Code Management
- Digital Assistant
- Digital Media
- Domain Name System (DNS)
- Email Delivery
- Events
- Exadata Cloud at Customer
- Exadata Cloud Service
- FastConnect
- File Storage
- Full Stack Disaster Recovery
- Functions
- Fusion Analytics Warehouse
- Fusion Apps as a Service (FAaaS)
- GoldenGate
- Health Checks
- Identity and Access Management
- Integration
- Java Management
- Language
- License Manager
- Load Balancer
- Logging
- Logging Analytics
- Managed Access
- Management Agent
- Marketplace – Consumer
- Monitoring
- MySQL Database

- NetSuite Health Check
- Network Firewall
- Network Load Balancer
- Network Path Analyzer
- Networking
- NoSQL Database
- Notifications
- Object Storage
- Operations Insights
- Operator Access Control
- Oracle Database Service for Azure
- Oracle Ksplice
- Oracle Open Data
- Oracle Search Cloud
- OS Management
- Process Automation
- Recovery Database Service
- Registry
- Resource Manager
- Roving Edge Infrastructure
- Search
- Search Service with OpenSearch
- Security Zones
- Service Connector Hub
- Service Manager Proxy Service
- Service Mesh
- Site-to-service VPN
- Speech
- Stack Monitoring
- Status Service
- Streaming
- Tagging
- Threat Intelligence
- Vault
- Vision
- Visual Builder Cloud
- Visual Builder Studio
- VMWare Solution
- Vulnerability Scanning
- Web Application Accelerator
- Web Application Farewell

3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[8].

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba[9].

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[9] https://scope-europe.eu

The Code has been officially approved in May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[11]. The robust and complex procedures and mechanisms can be reviewed by any third-party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[12]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set out by the supervisory authority pursuant to Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; proactively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

3.3 Multiple Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e., continuous, rigorous, and independent monitoring, an independent complaints' handling process, and finally any CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Controls Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications, their respective reports and by free text responses. Additionally, the CSP will have to provide a general overview of the

[10] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[11] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[12] https://eucoc.cloud/en/public-register/assessment-procedure/

functionalities, technical, organisational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognised standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third-party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g., by sample-taking and requesting further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided that over a due period every Control will be subject to scrutiny by the Monitoring Body. Where applicable, aspects of current attention at the time of assessment shall be covered too, e.g., where such aspects were indicated in media reports, publications or actions of supervisory authorities.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indicating appropriate implementation by the Control Guidance, then, the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon, makes them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.11 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is, however, no difference in terms of which parts of the Code are covered, since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the "First Level of Compliance", Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body's report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms of providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third-party certificates and audit reports, that are recognised by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

Identical to the "Second Level of Compliance" but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognised standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is at the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[13] and referring to the Public Register of the EU Cloud CoC[14] to enable Customers to verify the validity of adherence.

4 Assessment of declared services by Oracle (see 2.)

4.1 Fact Finding

Following the declaration of adherence of Oracle Corporation (Oracle Cloud Infrastructure) ('**Oracle**'), the Monitoring Body provided Oracle with a template, requesting Oracle to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal[15], the Monitoring Body requested from Oracle a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Oracle a comparison of the declared Cloud Services of last year and this year as well as to explicitly indicate any Cloud Services that are no longer included in the Declaration of Adherence and, where applicable, provide the Monitoring Body with adequate reasons. To the extent the list of Cloud Services was extended, the Monitoring Body requested a confirmation, that any such additional Cloud Services are subject to the same technical, organisational and contractual framework as the original Cloud Services.

Oracle promptly responded to the templates. Information provided consisted of references and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable. This information was completed by the two confirmations requested by the Monitoring Body as well as a detailed comparison of the declared Cloud Services between last year and this year verification highlighting the changes and the reasons for them.

---

[13] https://eucoc.cloud/en/public-register/levels-of-compliance/
[14] https://eucoc.cloud/en/public-register/
[15] You can access the Verification Report(s) of previous year(s) via the following link(s): Report 2022

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[16], the Monitoring Body analysed the responses and information provided by Oracle.

Oracle's declared services have been externally certified and audited. Oracle holds an ISO certificate, which is valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services. The declaration of adherence referred to the respective ISO certification within the responses to Section 6 of the Code (IT Security). As provided by the Code, the Monitoring Body may consider third-party certifications and audits. Accordingly, the Monitoring Body verified the certification and references. Further in-depth checks were not performed, as provided third-party certifications adequately indicated compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Oracle which outlined how all the requirements of the Code were met by Oracle's implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of Controls from the Code for in-depth scrutiny. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information. The Controls selected for this level of review were: 5.1.A, 5.1.C, 5.1.D, 5.1.E, 5.2.E, 5.3.E, 5.4.A, 5.4.E, 5.4.F, 5.5.C, 5.5.D, 5.7.B, 5.10.B, 5.11.B, 5.12.G, 5.13.A, 5.13.B, 5.14.B, 5.14.F and 6.1.C.

4.3.2 Findings by the Monitoring Body

During the process of verification, Oracle consistently prepared the Declaration of Adherence well and thoroughly. Oracle's responses were detailed and never created any impression of intentional non-transparency. Requests for clarification, additional and supporting information, as well as relevant samples were promptly dealt with and always met the deadlines set by the Monitoring Body.

Related to the Monitoring Body's requests (see section 4.1), Oracle indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual framework. Where additional Cloud Services were added, Oracle provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

[16] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

A first area of focus was built around subprocessor management. Oracle has a defined mechanism to notify Customers of the changes in subprocessors. The timelines for objection and/or exercising an alternative option, as well as the means to do so were confirmed by Oracle 's contractual documents.

In the same vein, Oracle has implemented a review process for its subprocessors to ensure that they adhere to Oracle's privacy, security and compliance standards, and the whole process is overseen by a specific team. The list of subprocessors is made available to Customers through an internal tool or can be requested from a dedicated point of contact.

The Monitoring Body assessed Oracle's mechanisms for the transfer of personal data to third countries. Oracle relies on Adequacy Decisions, its Binding Corporate Rules for Data Processors (BCR-P) and the Standard Contractual Clauses (SCCs) for such transfers. Oracle provided a written confirmation that SCCs are applied on an overarching basis and that should other mechanisms of transfer be invalidated (e.g., BCR-P), the SCCs would continue to apply by default.

Customers' Audit Rights were also assessed. Oracle publishes its audit reports periodically, which can be downloaded directly through the Cloud console or may be requested from a dedicated point of contact. Customers' Audit Rights are a standard part of Oracle's DPA. Oracle's costs determination and allocation related to Customers' Audit Rights was also presented to the Monitoring Body.

Another area of focus has been the enablement of Customers, with respect to responding to Data Subject Requests. Customers are provided with the possibility to do so through self-service functionalities. The features are outlined in relevant documentation which is made available to Customers through Oracle's public website, as well as within internal tools. In addition to this, Oracle confirmed that where Customers require assistance, they may do so by creating tickets within a browser-based interface or through a dedicated Portal.

Policies to maintain an appropriate media disposal and data wiping governing storage media no longer in use were reviewed by the Monitoring Body. Such policy included the relevant procedures and steps taken by Oracle, including the teams involved, to ensure that data is securely overwritten or otherwise sanitised before reuse or disposal.

Relevant policies and procedures have also been established by Oracle to timely and adequately report data breaches to Customers without any undue delay. Oracle has also confirmed the dedicated channels through which such notifications are provided and the internal team responsible to overseeing that such notification takes place effectively.

5 Conclusion

The information provided by Oracle were consistent. Where necessary, Oracle gave additional information or clarified their given information appropriately.

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 1. The service(s) will be listed in the Public Register of the EU Cloud CoC[17] alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by Oracle to support the compliance of its service, the Monitoring Body grants Oracle with a Second Level of Compliance.

6 Validity

This verification is valid for one year. The full report consists of 12 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[18].

Verification-date: August 2023 **Valid until**: August 2024

Verification-ID: 2022LVL02SCOPE4214

[17] https://eucoc.cloud/en/public-register/
[18] https://eucoc.cloud/en/public-register/