Verification of Declaration of Adherence

Declaring Company: Oracle Corporation

Verification-ID	2022LVL02SCOPE4215
Date of Approval	November 2022
Valid until	November 2023

Table of Contents

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 being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC – at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers – was developed against Directive 95/46/EC[4] and incorporates 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

Oracle Fusion Cloud Enterprise Resource Planning[6] family products is a cloud-based ERP software application suite that enables customers to manage enterprise functions including accounting, financial management, project management and procurement.) [7]

2.1 Oracle Fusion ERP Cloud Service

- Enterprise Resource Planning
- Enterprise Resource Planning for Self Service
- Risk Management
- Financial Reporting Compliance
- Accounting Hub Service
- WebCenter Forms Recognition
- CPQ for ERP
- Payroll for ERP for United States
- Payroll for ERP for United Kingdom
- Subscription Management for ERP (Professional User)
- Subscription Management for ERP (Self-service User)

2.2 Oracle Fusion Supply Chain Management Cloud Service

- Order Management
- Product Management
- Product Management Reviewer
- Supply Chain Execution
- Supply Planning

[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/erp/
[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.

- Demand Management
- Sales and Operations Planning
- Fusion Enterprise Contracts
- Fusion Service Contracts
- Supply Chain Collaboration

2.3 Oracle Fusion Procurement Cloud Service

- Procurement
- Procurement Self Service
- DataFox Supplier Intelligence

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].

The Code has been officially approved May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body 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 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; pro-actively 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

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

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 Control's Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications and their respective reports or by free text. Additionally, the CSP will have to provide a general overview on the functionalities, technical and organizational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognized 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 request for 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 indications for 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 recognized 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 recognized 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 up to 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 refer 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**'), the Monitoring Body provided Oracle with a template, requesting Oracle to detail its compliance with each of the Controls of the EU

[13] https://eucoc.cloud/en/public-register/levels-of-compliance/
[14] https://eucoc.cloud/en/public-register/

Cloud CoC. Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a "service family". A service family requires that all services rely on the same core infrastructure, with regard to hardware and software, and are embedded in the same contractual framework.

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[15], the Monitoring Body analysed the responses and information provided by Oracle.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Oracle which outlined how all the requirements of the Code were met by Oracle 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.F, 5.2.B, 5.2.E, 5.3.C, 5.3.D, 5.4.B, 5.5.D, 5.5.E, 5.7.A, 5.7.D, 5.7.E, 5.8.A, 5.8.B, 5.9.B, 5.10.A, 5.11.C, 5.14.A, 5.14.F, 6.1.A, 6.2.H, 6.2.I and 6.2.P

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.

A first area of focus related to the understanding of the service family, and the related technical, organisational and contractual framework. This assessment came along with the understanding of the relevant public and internal references to the Cloud Services being declared adherent. Oracle provided relevant information allowing the Monitoring Body to conclude that the declared services, indeed, qualify as one Cloud Service Family.

Additionally, the Monitoring Body paid attention to appropriate procedures and sufficient enablement of Customers. One field of assessment has been the Customers' data deletion capabilities during the

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

period of provision of services. Customers are provided with self-service features, such as the possibility to delete the interface objects, as well as a menu option to remove personal data. Data retrieval can also be promptly initiated upon termination of the services. Customers have a set period for data retrieval.

The Monitoring Body assessed Oracle's mechanisms for the transfer of personal data to third countries. Oracle uses Binding Corporate Rules and Standard Contractual Clauses. Whilst Binding Corporate Rules are used as a safeguard for intra-group data transfers, Standard Contractual Clauses are used as a safeguard for all inter-group data transfers, including for transfers to non-EEA third party subprocessors.

Further to this, the procedures related to Customers' Audit Rights were assessed. The assessment focused on Oracle's methodology to determine the costs of audits, as well as the possibility for Customers to request additional evidence of compliance. Oracle provided the Monitoring Body with an overview of the methodology to determine the costs of an audit. Customers are also provided with the relevant communication channels to request additional evidence of compliance, beyond exercising its audit rights.

Oracle's records of processing activities ('**ROPA'**) built another area of focus. Oracle maintains a ROPA for all Lines of Business. In addition to this, the relevant communication channels for Customers providing the relevant information in relation to the completion and relevancy of the ROPA were confirmed by Oracle.

Oracle's personnel undergo mandatory training on how to handle Customer Personal Data, based on the employees' dedicated role and responsibility. In the same vein, technical, organisational and administrative controls are implemented by Oracle to restrict access to Customer Personal Data.

The declared services have been externally certified and audited. Oracle currently holds an ISO:IEC 27001:2013 certificate, 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 27001 certification within its responses to Section 6 of the Code (IT Security). As provided by the Code, the Monitoring Body may consider third party certifications and audits, during its assessment. Accordingly, the Monitoring Body did verify the certification and references.

Finally, the Monitoring Body assessed Oracle's Incident Reporting and Response Policy, which defines escalation paths depending on the incident. Relevant teams work in collaboration to determine whether a security breach potentially resulted in a Data Breach so follow ups can be done accordingly.

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 services will be listed in the Public Register of the EU Cloud CoC[16] 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 10 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[17].

Verification-date: November 2022 **Valid until**: November 2023

Verification-ID: 2022LVL02SCOPE4215

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