Verification of Declaration of Adherence

Declaring Company: Oracle NetSuite Inc.

Verification-ID	2021LVL02SCOPE218
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 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

Oracle NetSuite Inc. declared its Cloud Service Family "NetSuite"[6] adherent to the Code. The Cloud Service Family comprises of the following Cloud Services.

Oracle NetSuite business management application suite provides an integrated solution for running the core functions of a business, enabling seamless cross-departmental business process automation, and real-time monitoring of core business metrics. Businesses can deploy the solution as a business management suite or deploy specific applications that can be integrated with existing application investments. [7]

2.1 Platform/ Infrastructure

- Sandbox
- SuiteAnalytics Connect (ODBC)
- SuiteCloud Plus (SC+)

2.2 CRM +

- Premium Customer Center

2.3 SuitePeople

- SuitePeople HR

2.4 PSA

- Resource Allocation
- Advanced Projects
- Job Costing

[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.netsuite.com/
[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.

2.5 ERP / CORE

- Revenue Management
- CRM - SFA
- CRM - Marketing
- CRM - Support
- Adv Revenue Management
- Contract Renewals
- SuiteBilling
- Electronic Bank Payments
- Adv Procurement
- Financial Management - GL
- Financial Management - AP
- Financial Management - AR
- Fixed Assets
- Dunning Letters
- OneWorld
- PBCS (Analytics)
- Basic Projects
- Inventory
- Adv Inventory
- Adv Mfg: Adv Ship Notice
- Adv Mfg: Batch Process
- Adv Mfg: Discrete
- Adv Mfg: Quality Management
- Manufacturing WIP And Routings
- Incentive Compensation
- Demand Planning
- Adv Order Management
- WMS
- Work Orders & Assemblies
- Grid Order Management
- Quality Management
- Sales Orders
- Purchase Orders
- Time Tracking
- Expenses
- Advanced Financials
- Electronic Invoices
- Advanced Software

2.6 SuiteCommerce

- Site Builder
- Adv Partner Center
- SuiteCommerce Standard
- SuiteCommerce Advanced (SCA)
- SuiteCommerce Instore (SCIS)

2.7 Open Air

- Timesheet
- Expense management
- Project Management
- Resource Management
- Billing/Invoicing
- Budgeting
- Automatic Backup Service
- Dashboards and Reports
- OpenAir Connect/Integration Manager
- XML/SOAP API
- Business Intelligence Connector
- Mobile
- Projects Connector
- Revenue Recognition
- Multi-currency
- Document management
- Purchases management
- Outlook Connector
- Revenue Recognition
- Sandbox
- OpenAir/NetSuite Connector

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 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

[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/

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 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 NetSuite (see 2.)

4.1 Fact Finding

Following the declaration of adherence of Oracle NetSuite Inc. ('**Oracle NetSuite**'), the Monitoring Body provided Oracle NetSuite with a template, requesting Oracle NetSuite 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 NetSuite 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 NetSuite a comparison of the declared Cloud Services of last year and this year as well as to explicitly indicate any Cloud Services that

[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): Verification Report 2021

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 NetSuite 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.

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 NetSuite.

Oracle NetSuite's declared services have been externally certified and audited. Oracle NetSuite holds ISO 27001:2013 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 NetSuite which outlined how all the requirements of the Code were met by Oracle NetSuite'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.C, 5.1.D, 5.1.F, 5.2.C, 5.3.A, 5.3.B, 5.3.D, 5.3.F, 5.4.A-B, 5.4.D, 5.5.A, 5.5.E, 5.8.A, 5.9.B, 5.11.B-C, 5.12.A-D, 5.13.A-B, 5.14.A-B, 5.14.E, 5.14.F and 6.1.A.

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

4.3.2 Findings by the Monitoring Body

During the process of verification, Oracle NetSuite consistently prepared the Declaration of Adherence well and thoroughly. Oracle NetSuite'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 NetSuite indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual framework.

The Monitoring Body assessed Oracle NetSuite's management of its subprocessors. Oracle NetSuite notifies customers of changes in its subprocessors, by sending email notifications to impacted customers. Alternatively, Customers who have access to the My Oracle Support portal can also sign-up to get the notification automatically. Oracle NetSuite has a dedicated team in charge of such notification process. Oracle NetSuite also has an internal tool to record Customers' objection and/or rejection of new subprocessors.

Another area of focus was around transfer of Customer Personal Data to third countries. Oracle NetSuite incorporates several mechanisms to safeguard third country transfers, of which Standard Contractual Clauses (SCCs) will stand ready in any case. In cases where transfers are subject to other mechanisms, next to SCCs (e.g., Binding Corporate Rules (BCRs)), such mechanisms will take precedence. For instance, BCRs are relied upon as a safeguard for intra-group transfers, whilst SCCs are used as a safeguard for transfer that do not qualify under previous category. Where Customer Audit Rights are concerned, the Monitoring Body reviewed the contractual agreements of Oracle NetSuite, as well as the methodology for cost determination. Previous audit reports are made available to Customers. Oracle NetSuite also makes itself available to respond to questions, at no charge. Where a customer wishes to exercise its audit rights, the latter has the option to request Oracle NetSuite's assistance in such audits, subject to a fee transparently communicated to Customers.

An overview of the key elements of the procedure to respond to requests from supervisory authorities was provided by Oracle NetSuite. Requests from supervisory authorities are managed and coordinated by Oracle NetSuite's Privacy Office. The procedures in place ensure that the requests are processed within an appropriate timeframe.

Oracle NetSuite has implemented policies and procedures to guide its personnel in reporting privacy and security incidents. These procedures are also communicated to Oracle NetSuite customers through a dedicated portal, i.e., public Security Incident Response website.

Another area of focus built around the sufficient enablement of Customers. During and after the terms of services, retrieval and deletion of Customer Personal Data may be autonomously done by Customer, through self-service functionalities or via customer request through Customer Support. Customers have up to 90 days to retrieve their data after the termination of their services.

Finally, the Monitoring Body scrutinised the data disposal policies and procedures of Oracle NetSuite, which aim to guide Oracle NetSuite's personnel on the disposal of Customer Personal Data. As per the provided responses of Oracle NetSuite, Oracle NetSuite has implemented mechanisms ensuring that Customer Personal Data will be disposed of in accordance with Oracle NetSuite's commitments, which might include regular (e.g., periodic) reviews.

5 Conclusion

The information provided by Oracle NetSuite were consistent. Where necessary, Oracle NetSuite 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 NetSuite to support the compliance of its service, the Monitoring Body grants Oracle NetSuite 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].

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

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

Verification-ID: 2021LVL02SCOPE218