SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Workday, Inc. and Workday Limited

EU CLOUD COC

Verification-ID	2019LVL02SCOPE001
Date of Approval	August 2022
Valid until	August 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[6]

2.1 Human Resources

- Learning
- Payroll
- Recruiting
- Time Tracking
- Talent Optimization

2.2 Finance

- Expenses
- Grants Management
- Procurement
- Projects
- Inventory
- Professional Services Automation
- Accounting Center

2.3 Enterprise Planning

- Financials Planning
- Financial Performance Management (FPM)
- HCM Planning (For Workforce Management)

[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://workday.com

2.4 Analytics and Reporting

- Workday Prism Analytics

2.5 Innovation Services

- Benchmarking
- Advanced Benchmarks
- Public Data
- Workday Graph (Skills Cloud)
- Journal Insights
- Workday Assistant
- HCM ML (GA)
- Learner Name
- Notification Designer
- Workday Journeys
- Content Cloud
- User Experience Machine Learning for Available Services
- Natural Workspaces
- Workday Extend
- Workday Student
- Workday Media Cloud

2.6 In-scope Workday Adaptive Planning Products:

- Workday Adaptive Planning

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[7].

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[8].

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

The Code has been officially approved May 2021[9]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[10]. 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.[11]

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 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.

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

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 consid-

ered 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[12] and refer to the Public Register of the EU Cloud CoC[13] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Workday, Inc. and Workday Limited ('**Workday**'), the Monitoring Body provided Workday with a template, requesting Workday to detail its compliance with each of the Controls of the EU 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.

Workday promptly responded. Information provided for each Control consisted of a reference to the Workday internal controls, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable.

As this declaration of adherence is a renewal[14], the Monitoring Body also requested from Workday a comparison of the declared services of last year and this year. The Monitoring Body also requested to

[12] https://eucoc.cloud/en/public-register/levels-of-compliance/
[13] https://eucoc.cloud/en/public-register/
[14] Download and access reports of prior assessments: Verification Report 2019, Verification Report 2020, Verification Report 2021.

explicitly indicate, any services that are no longer included in the declaration of adherence and, where applicable, provide the Monitoring Body with adequate reasons.

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 Workday.

Workday declared services have been externally certified and audited, e.g. Workday holds current SOC 2, ISO 27001 and 27017 certificates. The declaration of adherence referred to the respective ISO 27001 audit report 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 did verify the certification and references. Further in-depth checks were not performed, as provided third party certifications adequately indicate compliance. Controls were selected for an in-depth assessment based on several aspects, such as applied changes since the last assessment, ambiguities in responses, current relevant matters from a general data protection point of view.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Workday which outlined how all the requirements of the Code were met by Workday 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.E, 5.3.D, 5.3.F, 5.4.A, 5.4.E, 5.5.E, 5.5.F, 5.7.B, 5.7.C, 5.8.B, 5.9.A, 5.9.B, 5.11.B, 5.11.C, 5.12.A, 5.12.B, 5.12.G, 5.13.A, 5.14.A.

Compared to prior assessments, Workday has updated the list of Cloud Services that are subject to this verification. The Monitoring Body requested information and confirmation that any additional services rely on the identical frameworks as already verified services in prior assessments. Consequently, and following Workday's confirmation, especially as provided third-party certifications and reports are covering similar or even identical scopes as this verification, the Monitoring Body was able to transfer its prior findings and understandings to those additional services.

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

4.3.2 Findings by the Monitoring Body

Workday prepared this renewal well. Information was provided promptly following Monitoring Body's requests. The Monitoring Body never had the impression of non-compliance or deliberately ambiguous or misleading responses. Against this background, the Monitoring Body wants to contextualize the selection of Controls in this renewal: since the last renewal, the responsible department within Workday, which manages Declarations of Adherence towards the EU Cloud CoC, was restructured. Consequently, responses subtly deviated in style and language compared to previous years. The Monitoring Body sought to clarify those minor differences in approach, even though there was no suggestion of non-compliance

Given that the initial assessment of Workday dates to 2019, the Monitoring Body also examined already assessed elements. Against this background, the Monitoring Body assessed in more detail the flow-down mechanisms in regards to subprocessors. The Monitoring Body requested samples of relevant provision of the agreements and the performed due diligence by Workday. Workday implements provisions ensuring that subprocessors will provide no less protective measures than those provided by Workday. Workday assesses their subprocessors performance, thus applying due diligence.[16]

In this context, the Monitoring Body was also interested in the notification of changes of subprocessors. Workday provides an up-to-date list of subprocessors via its website. This communication channel is the default channel, by which Customers can identify any changes. Additionally, Customers can opt-in to a pro-active notification mechanism. The Monitoring Body also assessed the data protection awareness programme, including confidentiality obligations, of Workday employees and contractors. Workday ensures that its employees and contractors pass a dedicated programme and are subject to confidentiality obligations.

In regards to third country transfers, Workday implements appropriate safeguards. Where necessary, those safeguards are being updated. This also implies mechanisms to properly identify applicable safeguards to Workday's transfers.

The Monitoring Body was also interested in the Customer Audit Right. Workday provides the option, especially where pro-actively provided certifications and attestations may not suffice for the needs of a Customer, that Customer may exercise their Customer Audit Right. The Customer Audit Right follows

[16] **NOTE:** This report covers the adherent Cloud Services by Workday, see Section 2. It covers the due diligence by Workday to properly select and monitor its subprocessors. This report does not make any claims or findings regarding any such subprocessor's compliance with the Code. Interested parties may refer to the Public Register to learn more about other entities' compliance with the Code.

a determined procedure which outlines the roles and responsibilities of the parties involved. Costs related to the Customer Audit Right can be imposed on the Customer. There was no indication that such costs will be prohibitive or excessive. Alongside the extensive communication by Workday in regards to its implemented measures, Customers will also receive relevant information and support in case they are interested in the processing of Special Categories of Personal Data.

Workday has also implemented procedures to adequately assist and respond in the context of data subject right requests and supervisory authority requests. Workday has appointed a Data Protection Point of Contact. It has also implemented processes that support the processing of requests by Workday, so that responses can be provided in due time and of sufficient quality. This includes, besides others, an internal escalation and involvement of relevant departments, as necessary.

Customers are also enabled to retrieve their Customer Personal Data, where needed, by self-service.

5 Conclusion

The information provided by Workday was consistent. Where necessary Workday 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 3.4.1.2and 3.4.2 and given the type of information provided by Workday to support the compliance of its service, the Monitoring Body grants Workday 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 the last page closes with the Verification-ID. Please refer to the table of contents at the top of this report to

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

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 2022 **Valid until**: August 2023

Verification-ID: 2019LVL02SCOPE001

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