SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Workday, Inc. and Workday Limited

EU CLOUD COC

Verification-ID	2019LVL02SCOPE001
Date of Approval	August 2021
Valid until	August 2022

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, the Code was developed against Directive 95/46/EC[4] 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

2.1 Human Resources

2.1.1 Learning[6]

2.1.2 Payroll

2.1.3 Recruiting

2.1.4 Time Tracking

2.2 Finance

2.2.1 Expenses

2.2.2 Financial Performance Management (FPM)

2.2.3 Grants Management

2.2.4 Procurement

2.2.5 Projects

2.2.6 Inventory

2.2.7 Professional Services Automation

2.3 Enterprise Planning

2.3.1 Financials Planning

2.3.2 HCM Planning (For Workforce Management)

2.4 Analytics & Reporting:

2.4.1 Workday Prism Analytics

[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] **Note:** The AWS environments utilized for Media Cloud (software, data, text, audio, video, images or any other content that the Customer submits as part of a learning campaign within the Workday Learning Service) and Benchmarking (non-tenanted, pseudonymized data) are not in-scope for this assessment.

2.5 Platform, Product Extensions, and Industry specific applications

2.5.1 Innovation Services

- Public Data
- Benchmarking
- Advanced Benchmarks
- Workday Graph (Skills Cloud)
- Journal Insights
- Workday Assistant

2.5.2 Workday Extend (formerly Workday Cloud Platform)

2.5.3 Workday Student

2.6 Workday Adaptive Planning Products

2.6.1 Workday Adaptive Planning

Further descriptions and details on each service can be found at Workday's website.[7]

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. SCOPE Europe has been officially accredited as Monitoring Body May 2021. 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.[10]

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

[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.
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[9] https://scope-europe.eu
[10] https://eucoc.cloud/en/public-register/assessment-procedure/

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 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 both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g., by media reports, publications and actions of supervisory authorities are covered.

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 make 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 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[11] and refer to the Public Register of the EU Cloud CoC[12] 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 by 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.

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[13], the Monitoring Body analysed the responses and information provided by Workday.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

This verification is a so-called renewal, i.e., Cloud Services declared adherent[14] have already been assessed and Workday has already undergone prior assessments[15] related to the Cloud Services declared adherent[16]. Consequently, the Monitoring Body strives to rely on findings of prior verifications.[17] Workday confirmed that there have been no updates related to the contractual or technical

[11] https://eucoc.cloud/en/public-register/levels-of-compliance/
[12] https://eucoc.cloud/en/public-register/
[13] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/
[14] See 2.
[15] Download and access reports of prior assessments: Verification Report 2019, Verification Report 2020.
[16] See 2.
[17] Download and access reports of prior assessments: Verification Report 2019, Verification Report 2020.

framework that would affect the understanding that Cloud Services declared adherent relate to one service family.

The Monitoring Body reviewed the 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, including but not limited to sample taking. The controls selected were: 5.1.D, 5.1.E, 5.3.G. 5.4.*[18], 5.6.A, 5.7.B, 5.7.E, 5.7.F, 5.11.C, 5.12.D, 5.12.F, 5.12.G, 5.13.B, 5.14.E, 5.5.* and 6.2.* relating communication of available certifications and reports to Customers, and 6.2.L.

Based on the information provided by Workday, a follow-up request was made, for further detail on implemented measures related to Controls and respective information provided for: 5.4.*, 5.6.A, 5.7.E, 5.7.F, 5.12.G.

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. .

At the same time Cloud Services, respectively Cloud Service-related brand names, are not subject to this verification anymore that have been subject to prior verifications[19]: Following Workday's statements, this is a result of restructuring and (re-)merging functionalities and Cloud Service-related brand names, without effects on the actual measures as well as technical and organizational framework.

4.3.2 Findings by the Monitoring Body

Workday prepared its renewal. Consequently, requests by the Monitoring Body were responded in due time and with the expected level of quality and detail.

As the EU Cloud CoC has been officially approved prior to this renewal, the required communication of adherence and the related internal awareness of Workday's personnel has been in focus. Workday

[18] "*" indicates that the assessment either addressed all controls of the subsection or it addressed an aspect that is of cross-relevance to several / all controls of the subsection.
[19] Download and access reports of prior assessments: Verification Report 2019, Verification Report 2020.

convincingly referred to procedures safeguarding internal awareness. Workday also communicates its adherence to its Customers, e.g., via its Customer Portal.

Another priority in this year's assessment has been third country transfers. Following Workday's statements and provided documents, Workday does not transfer any Customer Personal Data based on Privacy Shield anymore. Following the publications of updated Standard Contractual Clauses for third Country Data Transfers (Standard Data Protection Clauses, Art. 46.2 f), short "SDPC") by the European Commission[20], Workday also convincingly outlined that it is currently amidst the process of evaluating and implementing the updated provisions by or before the required deadlines. Workday confirmed that it will notify the Monitoring Body once the implementation will be completed, allowing the Monitoring Body to further verify compliance with the updated SDPC.

Additionally, the Monitoring Body verified the measures implemented to support Customers in addressing data subject rights as well in retrieving their Customer Personal Data. Workday's responses indicated that Customers are able to retrieve their Customer Personal Data by so-called reports. These reports can be retrieved in several standard data formats. Workday indicated that Customers can access explanatory guidance on how to retrieve their Customer Personal Data via the Customer Portal, including possibilities to individually scope such reports as well as the technical processes and capabilities of such reports. Principally, Customer is considered to be enabled to address data subject right requests by self-service capabilities. To the extent Customer requests assistance, Workday convincingly referred to procedures adequately assigning related Customer-enquiries to specialised personnel / departments. Alongside the safeguarded expertise of personnel involved in assisting Customers, Workday prioritizes such enquiries ensuring timely responses. Workday safeguards that no unsuitable information is being shared for the purpose of assistance to data subject right enquiries, or any other assistance requested by Customers.

Related to the aforementioned, the Monitoring Body assessed whether and to which extent Workday implemented procedures to notify Customers in case of any supervisory authority requests. Workday clarified that it implemented a dedicated Data Protection Authority Request procedure, covering several aspects including Customer notification.

[20] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914.

Significant decisions and guidelines have been published recently, underpinning the need for appropriate internal training and other means to safeguard personnel's expertise. Consequently, one aspect of this verification has been related to the continuous updating of such internal training programmes. By functionality, Customers expect Workday's Cloud Services to be capable of processing Special Categories of Personal Data, whilst Monitoring Body acknowledges that Workday may not be aware of such processing in cases where Customers process Special Categories of Personal Data in non-predetermined contexts. Still, the Monitoring Body assessed if Customers will be able to adequately reach out to Workday requesting assistance on the implemented measures by Workday. Workday indicated that – also pre-contractually – Customer may file requests for such information according to its dedicated process for Data Protection Impact Assessment support. Against this background, Monitoring Body has been convinced that Customer will be sufficiently informed on the implemented measures to determine whether provided Cloud Services meet their individual requirements.

5 Conclusion

Given answers by Workday were consistent. Where necessary Workday provided 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[21] alongside this report.

In accordance with sections 3.4.1.2 and 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 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[22].

Verification-date: August 2021 **Valid until**: August 2022

Verification-ID: 2019LVL02SCOPE001

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