SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Workday Inc. and Workday Limited

EU CLOUD COC

Verification-ID	2019LVL02SCOPE001
Date of Approval	August 2026
Valid until	August 2027

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' or 'Code')**[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 (**'CSPs'**) – 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 Human Capital Management

Product SKUs

- Advanced Compensation Management
- Benefits
- CloudConnect for Benefits
- Core Human Capital Management
- Help
- Journeys
- Journeys for Activation
- Human Capital Management
- Talent Optimization
- Carrier Integrations by Benefit Harbor
- Pay Transparency Analyzer by Kainos

Innovation Services/Enhanced Features

- Help
- Journeys
- Ad Hoc Worker Communications

2.2 Financial Management

Product SKUs

- Accounting Center
- Core Financials

[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

- Expenses
- External Transaction Matching
- Financial Management Connector for Salesforce
- Financial Performance Management
- Grants Management
- Project Billing
- Projects
- Services CPQ
- Revenue Management
- Time Tracking
- External Transaction Matching by Trintech

Innovation Services/Enhanced Features

- Distance Calculation for Expenses
- Financial Management ML GA Features
- Receipt Scanning for Expenses
- Supplier Invoice Automation - Scanning
- SmartBots for Workday by Auditoria.AI
- Workday Bank Connectivity by Kyriba

2.3 Student

Product SKUs

- Workday Student Service
- Journeys for Student

Innovation Services/Enhanced Features

- Student Machine Learning Generally Available Features

2.4 Spend Management

Product SKUs

- Inventory
- Procurement

Innovation Services/Enhanced Features

- Spend Management ML

2.5 Payroll

Product SKUs

- Cloud Connect for Third Party Payroll
- Global Payroll Connect
- Payroll for Australia
- Payroll for Canada
- Payroll for France
- Payroll for United Kingdom and Ireland
- Payroll for United States
- DATEV Connector by SHAPEIN
- Global Payroll Services by Remote

- Payroll Services by OneSource Virtual (OSV)
- Payroll Services by Strada

Innovation Services/Enhanced Features

- Payroll Machine Learning Generally Available Features
- P45 Tax Form Scanning

2.6 Workforce Management

Product SKUs

- Absence Management
- Labor Optimization
- Scheduling
- Time Tracking Hub
- b-comm Time Clock Connector provided by dormakaba
- Smart Time Clock by NoahFace

Innovation Services/Enhanced Features

- Workforce and Pay ML
- Labor Optimization

2.7 Talent Management

Product SKUs

- Learning
- Cloud Connect for Learning
- Recruiting
- Succession Planning
- Talent Optimization
- Talent Optimization Add-On
- Workday Learning for Extended Enterprise
- Performance and Development
- Candidate Engagement

Innovation Services/Enhanced Features

- Human Capital Management ML GA Features
- Cloud Connect for Learning
- Public Learning Content
- Learner Name
- Recommended Interview Scheduling
- e-Commerce for Learning

2.8 Analytics and Reporting

Product SKUs

- People Analytics
- Prism Analytics

Innovation Services/Enhanced Features

- People Analytics

2.9 Adaptive Planning

Product SKUs

- Adaptive Planning
- Adaptive Planning and Consolidation
- Financial Planning
- Financial Planning and Consolidation
- Operational Planning
- Planning
- Workforce Planning

2.10 Platform and Product Extensions

Product SKUs

- Bring Your Own Key (BYOK)
- Extend
- Media Cloud
- Messaging
- Workday Cloud Platform
- Workday Government Cloud

Innovation Services/Enhanced Features

- User Experience Machine Learning for Available Services
- Workday Assistant
- Global Address Lookup
- Notification Designer
- Workday Graph
- Workday Everywhere
- Email Analytics
- Email Ingestion
- Intelligent Core
- SMS Multi-Factor Authentication
- Enterprise Search
- Workday AI Gateway
- Workday Orchestrate for Integrations
- Productivity Suite ML Features
- Global Address Validation
- Messaging
- Globalization Services Machine Translation (MT) Features
- Extend Integration with Third Party Platform Services

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[6].

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 SRL[7].

The Code has been officially approved in May 2021[8]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[9]. 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 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

---

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[7] https://scope-europe.eu
[8] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[9] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[10] 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[11] and referring 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 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.

As this declaration is a renewal[13], the Monitoring Body requested from Workday a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Workday a comparison of the declared Cloud

[11] https://eucoc.cloud/en/public-register/levels-of-compliance/
[12] https://eucoc.cloud/en/public-register/
[13] You can access the Verification Report of previous year via the following link: Workday - Verification Report – (2025)

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.

Workday 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 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[14], the Monitoring Body analysed the responses and information provided by Workday.

Workday's declared services have been externally certified and audited. Workday holds a current SOC 2 Report, 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 SOC 2 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 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 Workday which outlined how all the requirements of the Code were met by Workday'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.D, 5.1.E, 5.1.F, 5.1.H, 5.3.C, 5.3.D, 5.3.E, 5.4.A, 5.4.C, 5.4.D, 5.4.E, 5.5.A, 5.5.C,

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

5.5.E, 5.7.A, 5.7.E, 5.7.F, 5.8.A, 5.8.B, 5.10.A, 5.11.B, 5.12.A, 5.12.B, 5.12.C, 5.12.D, 5.12.G, 5.13.A, 5.13.B, 5.14.D, 5.14.E, 5.14.F and 6.1.C.

4.3.2 Findings by the Monitoring Body

During the process of verification, Workday consistently prepared the Declaration of Adherence well and thoroughly. Workday'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), Workday 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, Workday provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

Workday confirmed that a Cloud Service Agreement ("CSA") is in place between the CSP and its Customers determining the terms under which Workday shall process Customer Personal Data on behalf of the Customer, and the processing activities in relation to such data engaged in by the CSP and any subprocessor.

Workday indicated that its adherence to the Code is communicated to its personnel and that the latter is aware of the adherence to the Code in order to adequately handle related Customer inquiries. Specific trainings have been put in place by Workday to ensure its personnel is trained appropriately in this regard. Workday also publicly communicates its adherence to the Code on its Customer portal and Trust website.

The assessment involved the subprocessor management process. Based on the information provided by Workday, a process is in place to ensure that the CSP only engages subprocessors that can provide sufficient guarantees of compliance with the GDPR. This procedure considers different elements necessary for the evaluation of subprocessors, such as information security, corporate risk and privacy legal assessments. Workday has implemented procedures to ensure a flow-down of data protection obligations, and that appropriate technical and organisational measures no less protective than the ones provided by the CSP to the Customer are implemented by subprocessors. Moreover, Workday confirmed that a list of subprocessors with general information on the existing subprocessors and applicable jurisdictions is made available to the Customer through a dedicated website.

When it comes to third country transfers, Workday indicated that it relies on the appropriate data transfer safeguards as provided by Chapter V GDPR. The Monitoring Body received information from

the CSP confirming that it relies on its Binding Corporate Rules ("BCRs") and Standard Contractual Clauses ("SCCs"), of which the latter applies overarchingly. In addition, Workday confirmed that its privacy team monitors the applicability of existing adequacy decisions.

Workday confirmed that an up-to-date and accurate Record of Processing Activities ("ROPA") is maintained on behalf of Customers, including all information required under Article 30.2 GDPR. Also, Workday has established a support process that enables the Customer to provide relevant information, in order to keep the CSP's records of processing activities up-to-date and accurate.

Another area of focus was built around Data Subject Requests ("DSRs"). Workday has implemented self-service functionalities, which allow its Customers to independently handle DSRs. In this regard, Workday makes available support guides which outline how Customers can handle DSRs. Moreover, Workday has also established internal procedures that enable Customers to request support from CSP's dedicated contact points when assistance with handling DSRs is needed.

Workday confirmed that all employees and contractors are subject to appropriate confidentiality obligations before being engaged in data processing activities, which continue after the end of the employment or termination of the respective agreements. Workday requires personnel screening and mandatory training to ensure that employees and contractors involved in the processing of Customer Personal Data are aware of their confidentiality obligations.

In the context of data breaches, Workday provided information on its incident management policy and incident response plan, which are designed to identify, assess, handle and respond to data breaches, should any occur. Workday explained to the Monitoring Body the key aspects of these processes. The reporting of the data breaches to Customers is a contractual obligation, which is operationalised through relevant policies and procedures.

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[15] 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 15 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[16].

Verification-date: August 2026 **Valid until**: August 2027

Verification-ID: 2019LVL02SCOPE001

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