SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Workday Inc.

EU CLOUD COC

Verification-ID	2019PV02SCOPE001
Date of Approval	August 2020
Due date of Approval	August 2021

Table of Contents

1 Verification against v2.6 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 2.6 (**'v2.6'**)[2] as of March 2019.

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 v2.6 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

The EU Cloud CoC already applies the same principles and procedures now, pending the endorsement of the Code and its official approval by supervisory authorities, cloud service providers are welcomed and invited to sign up their services under v2.6 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

2 List of declared services

2.1 Human Resources

2.1.1 Workday Learning[6]
2.1.2 Workday Payroll
2.1.3 Workday Planning (For Workforce Planning)
2.1.4 Workday Recruiting
2.1.5 Workday Time Tracking

[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] excluding any software, data, text, audio, video, images or any other content from any source that the Customer submits as part of a learning campaign within the Workday Learning Service

2.2 Finance

2.2.1 Workday Expenses
2.2.2 Workday Financial Performance Management (FPM)
2.2.3 Workday Grants Management
2.2.4 Workday Planning (For Financial Planning)
2.2.5 Workday Procurement
2.2.6 Workday Projects

2.3 Analytics & Technology

2.3.1 Workday Benchmarking, an offering available as part of Workday Data-as-a-Service
2.3.2 Workday Prism Analytics
2.3.3 Workday Cloud Platform

2.4 Industry specific applications

2.4.1 Workday Inventory (For Healthcare)
2.4.2 Workday Professional Services Automation (for Professional Services Organization)
2.4.3 Workday Student (for Higher Education)

2.5 Innovation Services

2.5.1 Public Data
2.5.2 Benchmarking
2.5.3 Advanced Benchmarks
2.5.4 Workday Graph (Skills Cloud)
2.5.5 Journal Insights
2.5.6 Workday Assistant
2.5.7 Natural Workspaces
2.5.8 HCM Machine Learning Generally Available Features

2.6 Workday Adaptive Planning

2.6.1 Workday Adaptive Planning for Workforce Planning
2.6.2 Workday Adaptive Planning for Financial and Sales Planning
2.6.3 Adaptive Discovery

Any Cloud Services, upon and to the extent which those services are built – e.g. AWS – are not subject to this verification besides the appropriate subprocessor management by Workday.

3 Verification Process - Background

V2.6 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[7]. Those mechanisms will apply pending the formal approval of the EU Cloud CoC and accreditation of the Monitoring Body.

3.1 Provisional Status of the Verification Process

The services concerned passed a provisional verification process by the Monitoring Body of the EU Cloud CoC, i.e. SCOPE Europe sprl/bvba[8].

This provisional verification process follows the same principles and procedures as the EU Cloud CoC will apply under its official approval and accreditation. 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.[9]

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 and finally any

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

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

V2.6 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.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[10] and refer to the Public Register of the EU Cloud CoC[11] 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. ('**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, regarding hardware and software, and are embedded in the same contractual framework.

This verification is a so-called renewal, i.e. Cloud Services declared adherent[12] have already been assessed and Workday has already undergone prior assessments[13] related to the Cloud Services declared adherent[14]. Consequently, the Monitoring Body strives to rely on findings of prior verifications.[15] Workday confirmed that there have been no updates related to the contractual or technical

[10] https://eucoc.cloud/en/public-register/levels-of-compliance/
[11] https://eucoc.cloud/en/public-register/
[12] See 2.
[13] Download and access reports of prior assessments: Verification Report 2019.
[14] See 2.
[15] Download and access reports of prior assessments: Verification Report 2019.

framework that would affect the understanding that Cloud Services declared adherent relate to one service family. Compared to prior assessments, Workday has added some services to this verification. The Monitoring Body requested information and confirmation that additional services rely on the identical frameworks as already verified services in prior assessment, to be able to transfer its prior findings and understandings to those additional services.

At the same time Cloud Service are not subject to this verification anymore, that have been subject to the original verification[16]: Country specific brands of Workday Payroll, Time Tracking Hub, Cloud Connect for Benefits, Cloud Connect for Third Party Payroll, Human Capital Management, Workday Projects Billing, Core Financials. Functionalities and services seem to have restructured and remerged. The Monitoring Body has no reason to believe that this restructuring has any effect on the actual measures as well as technical and organizational 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[17], 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

The Monitoring Body reviewed the submission from Workday which outlined how all of 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.

This verification is a so-called renewal, i.e. Cloud Services declared adherent[18] have already been assessed and Workday has likewise undergone related prior assessments[19]. Consequently, one aspect of selection to be considered was whether Controls were already subject to prior assessments. As the Code were enhanced since prior assessments took place[20], another aspect of selection to be considered was whether such Code changes require a modified perspective or additional information to further rely on such prior verifications of related Controls.

---

[16] Download and access reports of prior assessments: Verification Report 2019.
[17] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/
[18] See 2.
[19] Download and access reports of prior assessments: Verification Report 2019.
[20] Assessment of Verification Report 2019 was against v2.2 of the Code. This verification is against v2.6.

The controls selected for this level of review were: 5.1.A, 5.1.D, 5.1.E, 5.1.I, 5.2.H, 5.3.B, 5.7.B, 5.7.D, 5.7.E, 5.7.F, 5.10.A, 5.11.A, 5.11.B, 5.11.C, 5.12.C, 5.12.D, 6.2.N.

Additionally, samples were requested regarding Controls: 5.3.C, 5.7.E, 5.7.F, 6.2.N.

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: 5.1.E, 5.1.I, 5.3.B, 5.10.A, 5.11.A, 5.12.D.

4.3.2 Findings by the Monitoring Body

Workday well prepared its renewal. Feedback and remarks provided within the initial assessment has been seriously taken into account. Consequently, requests by the Monitoring Body were responded in due time and with the expected level of quality and detail.

One area of focus in this assessment has been Workday's subprocessor management. Workday engages subprocessors based on a general authorization. Consequently, subprocessors may change during the performance of service. The Code requires – reflecting Article 28 GDPR – that changes to such subprocessors are to be duly notified to Customers, enabling Customers to effectively object such changes. Apparently, from the information provided, Customers will be duly notified about such changes. Workday's Cloud Service Agreement provides a multi-step approach regarding the possibility of Customers to object. This approach reasonably balances the interests of parties concerned, while keeping effective possibilities for Customers to prevent future subprocessors from processing Customer Personal Data. Besides, Customer may any time delete its Customer Personal Data or terminate the Cloud Service Agreement. Limitation to reasonability has been well reasoned: Especially taking into account the always existing possibility to delete Customer Personal Data, it is a fair balancing that Customers shall at least relate to data protection related concerns and not just perform their rights on occasion of such a change.

Cloud Services are usually built upon processing-chains. Consequently, an appropriate flow-down of rights and obligation is required by the Code. Based on the information provided by Workday it is apparent that rights and obligations are adequately flown-down.

In general, based on the information provided Workday services allow Customers to perform and process Customer Personal Data and related rights and obligations themselves. Workday offers assistance and support where needed. However, most of the times this will be general support as relevant information and tools are already accessible to Customers by default. Additionally, Monitoring Body

has been provided with documented procedures governing how Customers will be supported in case of need.

Internal enforcement of procedures has also been subject to this assessment. Workday responses convincingly assured that in cases Workday personnel, contractors or subprocessors are not compliant with contractual obligations, including policies and procedures, Workday will take appropriate and proportionate action. This is strongly supported by preventive measures such as training, internal evaluations, confidentiality agreements.

5 Conclusion

Given answers by Workday were 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[21] alongside this report.

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 2020 **Valid thru**: August 2021

Verification-ID: 2019PV02SCOPE001

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