SCOPE EUROPE

# Verification of Declaration of Adherence

Declaring Company: Workday Inc., Declaring Services: SAAS

EU CLOUD COC

| | |
|---|---|
| **Verification-ID** | 2019PV02SCOPE001 |
| **Date of Approval** | July 2019 |
| **Due date of Approval** | July 2020 |

# Table of Contents

# 1 Verification against v2.2 of the EU Cloud CoC

This Declaration of Adherence was performed against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] version 2.2 (**'v2.2'**)[2] as of March 2019.

Originally drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC (known as the C-SIG Code of Conduct on data protection for Cloud Service Providers) was developed against Directive 95/46/EC[4] incorporated feedback from 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, v2.2, its provisions have been aligned to the General Data Protection Regulation (**'GDPR'**)[5].

The EU Cloud CoC already applies the same robust principles and procedures now as it will in future, 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 v2.2 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

# 2 Verification Process - Background

V2.2 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 of the European General Data Protection Regulation[6]. Those mechanisms will apply pending the formal approval of the EU Cloud CoC and accreditation of the Monitoring Body.

## 2.1 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[7].

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

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.[8]

## 2.2 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 Cloud Service Provider with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body may request additional information. Where the information provided by the Cloud Service Provider appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

## 2.3 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 the deterrence of substantial remedies and penalties in case of any infringement.

## 2.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each Cloud Service Provider assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each Cloud Service Provider must detail 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 Cloud Service Provider may do so by either referencing existing third-party audits/certifications and their respective reports or by free text. Additionally, the Cloud Service Provider will have to provide

[8] https://eucoc.cloud/en/public-register/assessment-procedure/

a general overview on the functionality, technical and organisational controls and contractual frameworks of the service(s) declared adherent.

With regard 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 Cloud Service Provider applies to the Cloud Service concerned, (b) such third party certification or audit provided by the Cloud Service Provider 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 subsequent Recurring Assessment, the Monitoring Body will select an appropriate share of Controls such that over a suitable period every Control will be subject to scrutiny by the Monitoring Body. Some controls may be subject to increased attention as indicated e.g. by media reports or publications and actions of supervisory authorities.

If the responses of the Cloud Service Provider 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.

### 2.4.1 Levels of Compliance

A Cloud Service Provider is entitled to use the applicable Compliance Mark provided that the Cloud Service(s) declared adherent has been both verified compliant by the Monitoring Body and listed in the Public Register.

V2.2 of the Code provides three different ways to verify a Cloud Service Provider's compliance, so-called "levels of compliance". **It is important to note:** 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.

#### 2.4.1.1 First Level of Compliance

The Cloud Service Provider has performed an internal audit 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 Cloud Service Provider.

#### 2.4.1.2 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 Cloud Service Provider has undergone with regard 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 will 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. Cloud Service Providers 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 Cloud Service Provider 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 Cloud Service Provider.

#### 2.4.1.3 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 Cloud Service Provider has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards.

## 2.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[9] and refer to the Public Register of the EU Cloud CoC[10] to enable Customers to verify the validity of adherence.

# 3 List of declared services

The Workday Service consists of Workday Enterprise Cloud Applications:

## 3.1 Human Resources

### 3.1.1 Human Capital Management

### 3.1.2 Cloud Connect for Benefits

### 3.1.3 Workday Payroll for US

### 3.1.4 Workday Payroll for Canada

### 3.1.5 Workday Payroll for UK

### 3.1.6 Workday Payroll for France

### 3.1.7 Cloud Connect for Third Party Payroll

### 3.1.8 Workday Planning (For Workforce Planning)

### 3.1.9 Workday Time Tracking

### 3.1.10 Time Tracking Hub

### 3.1.11 Workday Recruiting

### 3.1.12 Workday Learning[11]

## 3.2 Finance

### 3.2.1 Core Financials

### 3.2.2 Workday Expenses

### 3.2.3 Workday Financial Performance Management (FPM)

### 3.2.4 Workday Grants Management

### 3.2.5 Workday Planning (For Financial Planning)

---

[9] https://eucoc.cloud/en/public-register/levels-of-compliance/
[10] https://eucoc.cloud/en/public-register/
[11] 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

Following the declaration of adherence of Workday Inc. (**'Workday'**), the Monitoring Body provided Workday with a template, requesting Workday to detail their 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 and extended the template with additional information to further demonstrate their compliance. Information provided for each Control consisted of at least a reference and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, a reference to Workday internal controls, a snippet of the relevant section of referenced Workday internal controls and a reference to third party audits and certifications, where applicable. This information was complemented by an overview of the actual structure of the service(s) declared adherent, describing the hardware and software and contractual framework, including the use of subprocessors.

Workday services are built on a multi-tenant architecture, in which Customer Personal Data is segregated logically. Customers share the same core-systems and may – within their logical environment

– configure defined deviations. The contractual framework is based on an overarching master agreement accompanied with sub-service specific addenda, where necessary.

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

Workday declared services are SOC 2 audited and ISO 27001, 27017 and 27018 certified. The declaration of adherence referred to respective audit report and/or certification within their 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.

As Workday provides a multi-tenant environment with logical segregation, the Monitoring Body did focus on implemented measures safeguarding that Customer Personal Data is not accessed by any customer other than the associated, legitimate customer.

As Workday transfers Customer Personal Data to third countries the Monitoring Body also focussed on measures implemented regarding safeguards of such transfers.

A key aspect of the EU Cloud CoC is, also, that Cloud Service Providers have to follow Customers instructions and need to cooperate with Customers in good faith, including possible audits. Declared service(s) by Workday are SaaS services. Hence, direct influence of Customers is limited by the type of service being offered, so the Monitoring Body focused on controls related to this key aspect of the Code.

## 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 of the requirements of the Code were met by Workday's control framework. In line with the Monitoring Body's process outlined in Section 2.4, the Monitoring Body selected a subset of controls from the Code for

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

in-depth scrutiny. The controls selected for this level of review were: : 5.2.C-E and F, 5.4.A-E, 5.5.A-B, 5.8.B, 5.12.A-C, 5.13.A-B, 5.14.C and 6.2.0.

Additionally, samples were requested regarding Controls: 5.2.H, 5.3.E, 5.5.D, 5.8.A, 5.12.D.

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: 5.2.D, 5.4.A and E, 5.5.D.

### 4.3.2 Findings by the Monitoring Body

During the process of verification, Workday consistently gave impression of having prepared the Declaration of Adherence well and thoroughly. Responses being provided were detailed and never created any impression of intentional non-transparency. Requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body.

The Monitoring Body did not focus on Section 6, as Workday provided an up to date SOC 2 report, as well as current ISO 27001/270017/270018 certifications, and referenced applicable sections of that report and those certifications to the Controls of the Code. The Monitoring Body may rely on such external reports and certifications, if those meet the criteria as set out in the Code, which is indicated where such international audit or certification is already being mapped within the Control's Catalogue. Referenced audits and certifications are those international standards, that have been appropriately mapped to Section 6, so that the Monitoring Body has strong indications allowing the Monitoring Body to rely those. Yet, the Monitoring Body analysed the report and certifications and assessed, whether the scope of applicability of them covered all Controls as provided by the Code, and where Controls were not covered, whether the scope of applicability provided reasons for non-applicability of such controls, that were consistent and convincingly accurate. Additionally, the personal data breach management is efficiently connected with the IT security incident management safeguarding appropriate detection, remediation and notification, where necessary.

Categories of personal data, that might be processed within the service(s) declared adherent, were not explicitly defined within the service agreement, but were not limited either. By the very nature of the service(s) and their related use cases for Customers, it is likely, that special categories of personal data will be processed. Consequently, all measures implemented by Workday consider the risk of processing as including special categories of personal data. In other words: the measures always seek to meet the protection requirements for sensitive data regardless whether Customers process

such sensitive data or not. This includes both personal data being processed by live systems and any associated backups.

Consequently, Workday supports all data being transmitted into their service(s) via encrypted channels. Browser-based applications as provided by Workday require the use of state-of-the-art encryption in transit to protect the communications between users and the Workday Service. Even other transmission channels, for transfer of data into or out of the Workday environment, require – by default – additional safeguard like PGP. Those additional safeguards may be deactivated by Customers but only by Customers designated security personnel, of which adequate expertise can be expected.

Logically segregated multi-tenant environments require sophisticated measures to ensure, that no data is unintentionally exposed to any customers other than the associated, legitimate customer. Workday elaborated on their measures, which can be considered as sophisticated. They comprise of multiple security layers, including firewalls and authorization and authentication, as well as a combination of several identifiers linked to each Customer, its users, and respective data being processed by that Customer. Lastly, personal data being processed is also subject to encryption at rest.

Customers may, always, access diverse information to address their need of transparency and enable them to ensure their own (Customers') compliance with GDPR. Via the so-called 'Workday Community", Customers may access information on implemented technical and organisational measures, third party certifications and audits, and further documentation. Whereas a lot of information can be accessed by any user, access is limited the more sensitive the information being provided in such documents becomes. Most of the documents can be freely accessed by respective, registered contact persons of Customers, whilst some documents will only be provided upon request and under a non-disclosure agreement. Where the provided information is not sufficient for the purpose of request of a Customer, the Customer may perform an individual audit, following a default audit plan. The measures presented to the Monitoring Body meet the requirements of the EU Cloud CoC.

Regarding management of subprocessor and third country transfers, Workday has implemented adequate measures. Regarding subprocessors Workday provided information on both adequate subprocessing agreement providing a level of data protection no less protective than Workday and the Code and continuous monitoring of subprocessors' compliance with their agreements. **For the avoidance of doubt:** this verification only assessed measures implemented by Workday and not of any of engaged subprocessors.

The subprocessors engaged were primarily Workday entities and Amazon Web Services, where Customer selects this option. Against this background, the Monitoring Body did have no reason to believe,

that implemented measures by subprocessors were in conflict with the measures described and guaranteed by Workday.

Regarding third country transfers Workday provided adequate information that any transfer of personal data is subject to at least one safeguard as provided by Chapter V of GDPR. Workday also described measures which ensure review of those transfers and related safeguards.

Employees are subject to confidentiality agreements and ongoing and adequate training, to ensure that implemented and described measures stay effective.

# 5 Conclusion

The responses by Workday were consistent. Where necessary, Workday provided additional information or clarified their responses and / or provided information appropriately.

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in section 4 above. The service(s) will be listed in the Public Register of the EU Cloud CoC[13] alongside this report.

# 6 Validity

This approval 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[14].

**Verification date**: July 2019 **Valid thru**: July 2020

**Verification-ID**: 2019PV02SCOPE001

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