SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Cisco International Limited

Verification-ID	2021LVL02SCOPE217
Date of Approval	October 2022
Valid until	October 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, 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 Webex[6]

Webex by Cisco is an enterprise solution for video conferencing, online meetings, screen share, and webinars. Webex Suite is the first, comprehensive suite for hybrid work consisting of services such as Calling, Meetings (i.e. Webex Meetings), Messaging (i.e. Webex and Webex App), Slido and Webex Events (formerly Socio).[7]

In scope of the Assessment has been the Webex Cloud Service Family with its Meetings and Messaging components, i.e.,

- Webex Meetings
- Webex
- Webex App[8]
- Webex Calling

[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://www.webex.com/
[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] The interface of Webex App, thus the cloud-run features, is in scope of the cloud service environment, thus subject to the Code and in the scope of the declaration of adherence. However, the mere client related matters of Webex App, i.e., local runtime environments etc., is not reflecting a cloud service, thus not subject to the Code and consequently out of scope of this declaration of adherence.

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[9].

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[10].

The Code has been officially approved May 2021[11]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[12]. 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.[13]

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

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[10] https://scope-europe.eu
[11] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[12] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[13] 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

V2.11 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[14] and refer to the Public Register of the EU Cloud CoC[15] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Cisco International Limited ('**Cisco**'), the Monitoring Body provided Cisco with a template, requesting Cisco to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal[16], the Monitoring Body requested from Cisco a confirmation that there has been no material change to the applicable technical and organisational, including contractual, framework. The Monitoring Body also requested from Cisco a comparison of the declared services of last year and this year as well as to explicitly indicate any services that are no longer included in the

[14] https://eucoc.cloud/en/public-register/levels-of-compliance/
[15] https://eucoc.cloud/en/public-register/
[16] You can access the Verification Report(s) of previous year(s) via the following link(s): Verification Report 2021.

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 and organisation, including contractual, framework as the original Cloud Services.

Cisco promptly responded to the template. 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. Cisco provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual 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 Cisco.

Cisco declared services have been externally certified and audited, e.g., Cisco holds current SOC 2, ISO 27001 and 27018, and C5 certificates. The declaration of adherence referred to the respective ISO 27001 certification 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.

As this declaration is a renewal[18], the Monitoring Body considered its previous assessments and developments in relation to GDPR implementation since then, when selecting the Controls for this renewal.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Cisco which outlined how all the requirements of the Code were met by Cisco 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

[17] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/
[18] You can access the Verification Report(s) of previous year(s) via the following link(s): Verification Report 2021.

level of review were: 5.1.B to 5.1.E, 5.2.A, 5.2.B, 5.3.B, 5.4.E, 5.5.C, 5.5.E, 5.5.F, 5.12.A to 5.12.F, 5.13.A, 5.13.B and 6.2.P.

4.3.2 Findings by the Monitoring Body

The Monitoring Body wants to highlight that the renewal has been triggered in due time by Cisco. Responses were provided in accordance with requested deadlines. Nonetheless, the process was not completed within the validation period, as transparently communicated by the Public Register. The Monitoring Body was never of the impression that Cisco is not acting in compliance with the Code. Delays resulted from rather administrative factors, such as change of responsible departments and contact persons and subsequent ambiguities in responses.

During the process of verification, Cisco consistently 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.

Related to the Monitoring Body's requests (see section 4.1), Cisco indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical and organisational framework. Where additional Cloud Services were added, the Monitoring Body requested explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

CSPs shall transparently communicate its adherence to the Code. Relevant information is provided to Customers by a dedicated portal[19], including detailed product information and Privacy Data Sheets. Such sheets also communicate the adherence to the Code, alongside other media. In this vein of cooperation with Customers, Cisco addresses its means to support Customer with their obligations under Art. 28 GDPR by various means. One area of focus has been the Customers' possibility to object to sub processors. Customers receive due notice about, and may object to, the addition of any new sub processors. Sub processors that have been objected to will not process Customer Personal Data.

The Monitoring Body also reviewed Cisco's management of Third Country Transfers. Cisco safeguards any such transfers at a minimum by Standard Contractual Clauses. In case other safeguards are implemented – additionally to the Standard Contractual Clauses – their validity is monitored as well as their adequate enforcement.

[19] https://trust.cisco.com/

As a current and applicable ISO certification was provided, and 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. The Monitoring Body principally relates to Cisco's applicable and current ISO certification. The Monitoring Body additionally reviewed the interlink of Cisco's (Security) Incident Response Plan with a Data Breach Response Plan. Cisco indicated that relevant teams will be assigned in the processing of any incident. If Customer Personal Data might be affected, the respective legal and (personal) data protection teams are involved, safeguarding that the incident is processed in due quality, due time and followed-by any notifications, where necessary.

Where Customer Audit Rights are concerned, the Monitoring Body scrutinized Cisco's implementation of any potential costs and additional procedural requirements. As a rule, Cisco does not charge customers for the audits. Cisco determines the procedural elements of any Customer Audit according to a pre-determined procedure. To the extent Cisco will require Customer to bear any costs, such costs will be determined by a pre-determined methodology. Expected costs remain reasonable relative to the scope of audit. In distinct cases, e.g., where such audit follows a legal requirement– such as an authority's request – costs will not be imposed.

Regarding employee's and contractor's confidentiality obligations, Cisco incorporates relevant provision in its agreements.

5 Conclusion

Given answers by Cisco were consistent. Where necessary Cisco 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 services will be listed in the Public Register of the EU Cloud CoC[20] alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by Cisco to support the compliance of its service, the Monitoring Body grants Cisco with a Second Level of Compliance.

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

6 Validity

This verification is valid for one year. The full report consists of 11 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[21].

Verification-date: October 2022 **Valid until**: October 2023

Verification-ID: 2021LVL02SCOPE217

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