

Verification of Declaration of Adherence

Declaring Company: Cisco International Limited



EU
CLOUD
COC

Verification-ID	2024LVL03SCOPE5422
Date of Approval	June 2024
Valid until	June 2025

Table of Contents

1	Verification against v2.11 of the EU Cloud CoC	3
2	List of declared services	3
2.1	Webex	3
3	Verification Process - Background	3
3.1	Approval of the Code and Accreditation of the Monitoring Body	4
3.2	Principles of the Verification Process	4
3.3	Multiple Safeguards of Compliance	4
3.4	Process in Detail	4
3.4.1	Levels of Compliance	5
3.4.2	Final decision on the applicable Level of Compliance	7
3.5	Transparency about adherence	7
4	Assessment of declared services by Cisco (see 2.)	7
4.1	Fact Finding	7
4.2	Selection of Controls for in-depth assessment	8
4.3	Examined Controls and related findings by the Monitoring Body	8
4.3.1	Examined Controls	8
4.3.2	Findings by the Monitoring Body	9
5	Conclusion	11
6	Validity	11

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 drafted by the Cloud Select Industry Group³ (**'C-SIG'**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers – was developed against Directive 95/46/EC⁴ 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 Webex⁶

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 Cisco Cloud Service Family, i.e.,

- Slido
- Events

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 GDPR⁸.

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 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

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/bvba⁹.

The Code has been officially approved in May 2021¹⁰. SCOPE Europe has been officially accredited as Monitoring Body in May 2021¹¹. 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.¹²

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 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

⁹ <https://scope-europe.eu>

¹⁰ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf>

¹¹ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf>

¹² <https://eucoc.cloud/en/public-register/assessment-procedure/>

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 Mark¹³ and referring to the Public Register of the EU Cloud CoC¹⁴ 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.

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 (i.e., technical framework), and are embedded in the same organisational and contractual framework.

Cisco 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. Cisco provided

¹³ <https://eucoc.cloud/en/public-register/levels-of-compliance/>

¹⁴ <https://eucoc.cloud/en/public-register/>

information illustrating the actual structure of the services declared adherent and describing the technical, organisational and contractual framework.

Given this declaration of adherence reflects an Initial Third Level of Compliance verification, some specifics must be considered. In the context of a Third Level of Compliance, the Monitoring Body must ensure that all relevant findings are covered by an existing third-party attestation report, and that the reasons for such third-party assessor to conclude positively can be derived from such a third-party attestation report, mainly in Section 5. Consequently, the Third Level of Compliance is not incompatible with the Monitoring Body requesting additional information (see Section 4.3.1). The Monitoring Body will apply the process which is best suited to conclude on compliance with Code and the respective Level of Compliance.

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC¹⁵, the Monitoring Body analysed the responses and information provided by Cisco.

Cisco's declared services have been externally certified and audited. Cisco holds an ISO 27001 and 27701 certificates, 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 ISO 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 verified the certification and references.

To this extent, further in-depth checks were not performed, as provided third-party certifications adequately indicated compliance. Additionally, as this was a Third Level of Compliance verification, the Monitoring Body verified that every Control has been subject to a third-party assessment, either by recognized standards such as ISO or SOC, or a dedicated EU Cloud CoC related third-party attestation report. Alongside ISO and SOC statements, Cisco submitted a dedicated EU Cloud CoC related attestation report.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Cisco which outlined how all the requirements of the Code were met by Cisco's implemented measures. In line with the Monitoring Body's process

¹⁵ <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

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.A, 5.1.D, 5.1.H, 5.2.C, 5.2.F, 5.3.D, 5.4.E, 5.5.C, 5.7.D, 5.7.F, 5.8.A, 5.10.A-B, 5.12.A-B, 5.12.D-F, 5.14.B, 5.14.F and 6.1.D.

4.3.2 Findings by the Monitoring Body

During the process of verification, Cisco consistently prepared the Declaration of Adherence well and thoroughly. Cisco'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.

While this is a Third Level of Compliance verification, responses to every Control were supported by third-party attestations, including a dedicated EU Cloud CoC related attestation report. The dedicated report was prepared thoroughly by the third-party auditors. Requests for clarification, additional and supporting information, as well as relevant samples were promptly dealt with by the third-party auditors. The Monitoring Body has no reason to doubt the appropriate performance of the relevant third-party attestation, neither from a formal perspective nor from a material perspective, e.g., that a significantly diverse understanding of the Code has been applied.

The Monitoring Body verified that declared Cloud Services qualify both as Cloud Service under the Code and as Cloud Service Family. Related to the Monitoring Body's requests (see section 4.1), Cisco provided information outlining the structure of the services, contractual and supporting documents enabling the Monitoring Body to better understand Cisco's service offerings. Cisco provided explicit confirmation that all Cloud Services declared adherent belong to the same Cloud Service Family.

The Monitoring Body has focused on the information provided to the Customers. Cisco has indicated that a Cloud Service Agreement incorporating the data protection obligations under GDPR as a minimum, is in place with the Customer. The information with regards to data formats, processes, technical requirements and timeframes of retrieving the entrusted Customer Personal Data is provided to the Customer in the relevant contractual documents. Further, Cisco indicated that procedures are implemented to internally communicate its adherence to and the requirements of the Code, allowing its personnel to adequately deal with related customer inquiries.

Assistance provided to Customers was assessed by the Monitoring Body. As per internal procedures indicated by Cisco, Customers are provided with assistance to complete the Data Protection Impact Assessment (DPIA) and are enabled to retrieve their data both during and at the end of the provision

of the Cloud Services. Customers can access and export their data by utilizing the self-service functionalities provided by Cisco or by submitting request via a communication channel. In addition, self-service functionalities can be utilized by Customers to deal individually with data subject requests. To provide additional support where needed, Cisco indicated that a dedicated communication channel is maintained for the Customers.

The subprocessor management program was also in the scope of the assessment. The Cloud Service Agreement defines the processing activities in relation to Customer Personal Data engaged by Cisco and subprocessors. In this regard, Cisco has indicated that the subprocessor management policies and standards are implemented to ensure that the same data protection obligations and appropriate technical and organisational measures, as provided by Cisco to Customer, are implemented to the full subprocessing chain. Furthermore, such policies provide that appropriate agreements with subprocessors shall be executed, to ensure the flow down of the contractual requirements and its implementation.

The Monitoring Body has assessed the Customers' Audit Rights. According to the information provided by Cisco, a dedicated communication channel is available through public-facing website. By it means Customers can access the compliance information, including third-party audit reports and certifications, which can be accessed directly or made available upon request. Customer Audit Rights are incorporated as a standard provision of the contractual documents with Customers. This ensures that Customers can exercise their audit rights: by getting the relevant assistance, access to the compliance information, and requesting individual audits, including inspections.

The confidentiality obligations have also been a part of the assessment. As per Cisco's internal policies, the confidentiality obligations with employees and contractors are in place and continue after the end of the employment or termination of the respective agreements. When it comes to the training and awareness of personnel involved in the processing of the Customer Personal Data, Cisco provided information that mandatory awareness training program, covering such topics as data protection and privacy, is provided on a regular basis. Such training is specific to the role and job functions of the personnel, as it is provided per respective service lines, and is reviewed for completion and relevance.

Finally, third country transfers have been assessed by the Monitoring Body. In accordance with information provided by Cisco it relies on the appropriate data transfer safeguards as provided by Chapter V GDPR. For data transfers to a third country outside the EEA Cisco confirmed to rely on Adequacy decisions or to utilize such data transfer safeguards as Standard Contractual Clauses (SCCs).

5 Conclusion

The information provided 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 service(s) will be listed in the Public Register of the EU Cloud CoC¹⁶ alongside this report.

In accordance with sections 3.4.1.3 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 Third Level of Compliance.

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 CoC¹⁷.

Verification-date: June 2024

Valid until: June 2025

Verification-ID: 2024LVL03SCOPE5422

¹⁶ <https://eucoc.cloud/en/public-register/>

¹⁷ <https://eucoc.cloud/en/public-register/>