SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Cisco International Limited

Verification-ID	2024LVL03SCOPE5318
Date of Approval	February 2024
Valid until	February 2025

Table of Contents

1 Verification against v2.11 of the EU Cloud CoC 3

2 List of declared services 3

2.1 ThousandEyes Platform 3

3 Verification Process - Background 4

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 5

3.4.1 Levels of Compliance 6

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 Group[3] (**'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/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 ThousandEyes Platform [6]

ThousandEyes, the Internet and Cloud Intelligence company, delivers a collectively powered view of the Internet enabling enterprises and service providers to work together to improve the quality of every digital experience. The ThousandEyes platform leverages data collected from a fleet of vantage points throughout the global Internet, from within data centers and virtual private clouds (VPC) and on end user devices to expose key dependencies that impact digital service delivery, empowering businesses to see, understand and improve how their customers and employees experience any digital website, application, or service.[7]

On August 7, 2020, Cisco completed its acquisition of ThousandEyes.

In scope of the Assessment has been the ThousandEyes Cloud Service Family, i.e.,

- Cloud Agents;
- Enterprise Agents;
- Endpoint Agents;
- Internet Insights.

[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://app.thousandeyes.com/login
[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.

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[8].

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[9].

The Code has been officially approved in May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[11]. 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

---

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

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[13] and referring to the Public Register of the EU Cloud CoC[14] 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

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

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 the EU Cloud CoC related third-party attestation report drafted by the third-party assessor for CISCO, references to the relevant sections of the third-party attestation report and to third party audits and certifications, where applicable. CISCO provided information illustrating the actual structure of the services declared adherent and describing the technical, organisational 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[15], 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 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 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 Third Level of Compliance verification, both Sections 5 and 6 of the Code have been covered by the third-party assessors, either by recognized standards such as ISO or SOC, or a dedicated EU Cloud CoC related third-party 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 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-B, 5.1.D-E, 5.2.B-G, 5.3.D, 5.4.B-C, 5.4.E, 5.7.B, 5.7.F, 5.8.A, 5.10.B, 5.11.B, 5.12.B-C, 5.12.E, 5.14.A-C, 5.14.E, 6.1.A-B, 6.1.D and 6.2.I.

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

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 and where required the third-party assessor'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.

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. Furthermore, scope of the Cloud Services verified by the Monitoring Body were confirmed to be aligned with the scope examined by the third-party assessor.

Given this is an initial declaration of adherence and that CISCO was seeking for the Third Level of Compliance verification, some specifics were necessary to be considered. Given the Third Level of Compliance, the Monitoring Body must ensure, that all relevant findings mainly in Section 5 complied with and covered by an existing third-party attestation. Such attestation shall also include the reasons for such third-party to conclude positively. Consequently, the Third Level of Compliance is not incompatible with the Monitoring Body requesting additional information. The Monitoring Body will apply the process that best enables it to conclude on compliance.

Against this background, the Monitoring Body requested clarifications. The Monitoring Body never had any doubts of compliance by CISCO, but wanted to ensure that the provided third-party attestation is sufficiently clear to allow the Monitoring Body to draw its conclusions.

Where requested, the Monitoring Body received prompt response from CISCO and – where needed – from the third-party assessor who drafted the distinct EU Cloud CoC related third-party attestation.

The Monitoring Body has focused on the assistance and information provided to the Customers. CISCO has demonstrated that relevant contractual agreements incorporating the data protection obligations under GDPR as a minimum and not less protective as required by the Code are executed with the Customers. Further, information related to security, privacy measures and compliance is made available to the Customers by different means including privacy data sheets and trust portal. As indicated by CISCO, Customers are provided with various self-service functionalities covering data

subject requests (DSRs); deletion of Customer Personal Data; and retrieval and export of Customer Personal Data in machine readable, commonly used, structured format. Additionally, CISCO confirmed to have internal procedures to further assist Customers with DSRs; together with documentation webpages and guidelines to help Customers with the provided self-service functionalities. Finally, Customers may reach out via dedicated communication channels and trust portal if further assistance is required.

Third country transfers have also been assessed by the Monitoring Body, CISCO indicated that it relies on the appropriate data transfer safeguards as provided by Chapter V GDPR. It has been demonstrated that adequacy decisions and Standard Contractual Clauses (SCCs) alongside with the Binding Corporate Rules (BCRs) are relied upon to safeguard third country transfers. CISCO confirmed to continuously monitor whether the destination of a data transfer is subject to an adequacy decision of the European Commission.

Another aspect of the assessment involved CISCO's subprocessors management process. Based on the information provided by CISCO, relevant policies and procedures have been implemented to establish internal data protection and privacy requirements for engagement of the subprocessors. Furthermore, such policies and procedures indicated that appropriate agreements shall be executed with the subprocessors, ensuring at a minimum flow down of the same data protection obligations and appropriate technical and organisational measures as provided by CISCO to the Customer.

Training and awareness obligations with regards to employees and contractors were also part of the assessment. CISCO has confirmed that employees and contractors as per implemented internal policy are subject to obligatory regular privacy and security training. Such trainings are specific as to the role and functions of the employees and contractors. Moreover, CISCO has indicated that access management procedures and relevant policies are in place to ensure that Customer Personal Data is not processed by any personnel for any purpose independent of the Instructions of the Customer.

To the extent records of processing activities (ROPA) is concerned, according to the information provided, the Monitoring Body was able to conclude that CISCO maintains an up-do-date and accurate ROPA in its capacity as Processor, which includes the relevant information as per Article 30.2 GDPR. It has been indicated by CISCO that Customers are provided with self-service functionalities to provide and update the information in relation to the completion and relevancy of the ROPA.

Requests by supervisory authorities have also been in the scope of the assessment. Internal policies and procedures have been confirmed to be implemented by CISCO to respond to requests by supervisory authorities in due time and appropriate details and quality. Such requests are tracked internally

and undergo quality assurance review by relevant personnel, including privacy and legal experts. Additionally, CISCO's internal procedures verified that a specific timeline for such requests to be processed is established.

After assessing the provided third-party attestation report and the additional supplementary information received by the assessor upon request, 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. Additionally, based on the provided information the Monitoring Body concludes CISCO's compliance to the Code.

5 Conclusion

The information provided by CISCO was 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 CoC[16] 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 CoC[17].

Verification-date: February 2024 **Valid until**: February 2025

Verification-ID: 2024LVL03SCOPE5318

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