Verification of Declaration of Adherence

Declaring Company: Okta Inc.

EU CLOUD COC

Verification-ID	2022LVL02SCOPE3112
Date of Approval	July 2022
Valid until	July 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 Okta (Platform) Services[6][7]

The Okta platform services are foundational components that power Okta product features.[8]

The platform services and products subject to this declaration of adherence are:

Access Gateway
Adaptive Multi-Factor Authentication
Advance Server Access
API Access Management
Identity Governance
Lifecycle Management
Universal Directory
Single Sign-On
Workflows

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].

---

[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] **NOTE**: Any Free Trial services provided by Okta are out of scope of this declaration of adherence.
[7] https://okta.com
[8] **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.
[9] 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/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 regard 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 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

[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/

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 Okta (see 2.)

4.1 Fact Finding

Following the declaration of adherence of Okta Inc. ('**Okta**'), the Monitoring Body provided Okta with a template, requesting Okta 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, and are embedded in the same contractual framework.

Okta promptly responded within the template. The provided information 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. Okta provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual framework.

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

The Monitoring Body explicitly analysed whether there is a difference regarding (Platform) Services and Products. Okta convincingly explained that differences in nomenclature has no impact on the technical, organisational, or contractual framework but only supports better clustering of the Cloud Services in Okta's internal and external communication.

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[16], the Monitoring Body analysed the responses and information provided by Okta.

Okta declared cloud services subject to this declaration of adherence[17] have been externally certified and audited, e.g., Okta holds current ISO 27001 certificates. Notwithstanding other certifications[18], 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. Further in-depth checks were not performed, as provided third party certifications adequately indicate compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Okta which outlined how all the requirements of the Code were met by Okta 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, 5.1.C, 5.1.D, 5.1.E, 5.1.H, 5.2.D, 5.2.E, 5.2.F, 5.2.G, 5.3.B, 5.3.D, 5.3.G; 5.4.A, 5.4.B, 5.5.C, 5.5.D, 5.5.E, 5.5.F, 5.6.A, 5.7.A, 5.7.D, 5.7.E, 5.7.F, 5.8.A, 5.11.B, 5.11.C, 5.12.C, 5.12.D, 5.12.F, 5.12.G.

4.3.2 Findings by the Monitoring Body

The Monitoring Body verified that declared Cloud Services qualify both as Cloud Service under the Code and as a Cloud Service Family. During the process of verification, Okta consistently gave the

[16] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/
[17] As listed above in section 2.
[18] https://trust.okta.com/compliance/

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 a current and applicable ISO certification was provided. 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 on those. The Monitoring Body analysed the certifications and assessed whether the scope of applicability covered all Controls as provided by the Code. Upon request Okta confirmed that all Cloud Services being declared in this declaration of adherence are covered by the respective certificates.

One area of focus was the understanding of the contractual framework, i.e., the applicable Data Processing Addendum (DPA). Okta updated the Data Processing Addendum during the process, which required the Monitoring Body to ensure assessing the current and applicable version. In this context, Okta also provided reasons for non-applicability of the Verification Process to the Free Trial versions, whilst acknowledging that the GDPR related matters are considered the same.

An area of focus has been assistance of and control by Customers. Okta assists Customers where needed. Principally, Customers are provided with documentation and third-party attestations. Where the provided information may not suffice, Customers may reach out to Okta and request additional assistance. Likewise, Customers may instruct Okta. Okta has implemented procedures to ensure that instructions are being followed, including mechanisms to ensure that instruction are duly authorized.

In the context of instructions, the Monitoring Body analysed the management of subprocessors and related transparency. Okta has implemented due notification of Customers in case of any changes. Customers can object and take effective measures prior changes are implemented. Okta has implemented measures to apply due diligence regarding its subprocessors, safeguarding subprocessors apply no less protective measures as provided by Okta. In the same vein the Monitoring Body successfully requested information ensuring compliance with the confidentiality obligations of employees and subcontractors, in general.

An area of assessment has also been the possibility for Customers for perform their right to audit. In accordance with the Code, Okta implemented a staggered approach, i.e., Customers may first seek

for relevant information either by Customer Support, existing third-party attestation, and document review. As provided by the contractual framework, Customers may – ultimately and where needed – seek for additional information. The Monitoring Body assessed the procedures involved, as well as the expected costs for Customers. The procedures balance the interests of the involved parties, including the confidentiality and security of the data processing of other Customers. To the extent costs are involved, the Monitoring Body concludes that those are not designed to prohibit Customers from performing their due rights, but representing the expected complexities involved.

Regarding third country transfers, Okta relies on Standard Data Protection Clauses, also referred to as Standard Contractual Clauses, as published by the European Commission. Okta stays within the deadlines of implementing the updated version.

Customers are principally enabled to retrieve their data, where needed, as well as respond to data subject requests autonomously. However, in case of need, Okta provides assistance upon request, ensuring GDPR requirements will be met, in this context, the Monitoring Body also analysed whether Okta implemented procedures to adequately respond to requests by Data Protection Supervisory Authorities.

5 Conclusion

Given answers by Okta were consistent. Where necessary Okta 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[19] alongside this report.

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

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

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[20].

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

Verification-ID: 2022LVL02SCOPE3112

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