SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Google LLC

EU CLOUD COC

Verification-ID	2020LVL02SCOPE015
Date of Approval	December 2022
Valid until	December 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 – was developed against Directive 95/46/EC[4] and 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 Google Workspace

Google Workspace products provide multi-user collaboration. The products are comprised of communication, productivity, collaboration and security tools that can be accessed virtually from any location with Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with an Internet connection.[6]

- Admin Console
- Assignments
- Calendar
- Classroom
- Cloud Identity
- Cloud Search
- Contacts
- Currents
- Docs
- Drive
- Forms
- Gmail
- Google Chat
- Google Meet
- Google Workspace Migrate
- Groups
- Hangouts
- Jamboard
- Keep
- Mobile Device Management
- Sheets
- Sites (Classic)
- Sites (New)
- Slides
- Tasks
- Vault
- Voice

[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**: 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.

2.2 Google Cloud Platform

Google Cloud Platform provides Infrastructure as a Service ("IaaS") and Platform as a Service ("PaaS"), allowing businesses and developers to build and run any or all of their applications on Google's Cloud infrastructure. Users can benefit from performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model.[7]

- Access Approval
- Access Context Manager
- Access Transparency
- AI Platform Data Labeling
- AI Platform Neural Architecture Search (NAS)
- AI Platform Training and Prediction
- AlloyDB
- Anthos Config Management (ACM)
- Anthos Identity Service
- Anthos Service Mesh (ASM)
- API Gateway
- Apigee
- App Engine
- Artifact Registry
- Assured Workloads for Government
- AutoML Natural Language
- AutoML Tables
- AutoML Translation
- AutoML Video
- AutoML Vision
- BeyondCorp Enterprise
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Chronicle
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Data Fusion
- Cloud Data Loss Prevention
- Cloud Debugger
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Run for Anthos
- Cloud Scheduler
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision
- Cloud VPN
- Compute Engine
- Connect
- Contact Center AI
- Container Registry
- Data Catalog
- Database Migration Service
- Dataflow
- Datalab
- Dataproc

[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.

- Datastore
- Dialogflow
- Document AI
- Eventarc
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Game Servers
- Google Cloud Armor
- Google Cloud Identity-Aware Proxy
- Google Cloud Threat Intelligence for Chronicle
- Google Kubernetes Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- IoT Core
- Key Access Justification (Access Sovereignty)
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate for Compute Engine
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- Notebooks (formerly AI Platform Notebooks)
- Persistent Disk
- Pub/Sub
- reCAPTCHA Enterprise
- Recommender
- Resource Manager API
- Risk Manager
- Secret Manager
- Security Command Center
- Service Directory
- Service Infrastructure
- Speech-to-Text
- Storage Transfer Service
- Talent Solution
- Text-to-Speech
- Traffic Director
- Vertex AI (formerly AI Platform)
- Video Intelligence API
- Virtual Private Cloud (VPC)
- VPC Service Controls
- Web Risk API
- 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[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].

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

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

[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/

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 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 indications for 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 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 consid-

ered 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[13] and refer 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 Google (see 2.)

4.1 Fact Finding

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

Google 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 the measures, and a reference to third party audits and certifications, where applicable.

As this declaration is a renewal, the Monitoring Body requested from Google a confirmation that there has been no material change to the applicable technical, organisational and contractual framework. The Monitoring Body also requested from Google 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 declaration of adherence, and, where applicable, provide the Monitoring Body with adequate reasons.

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

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, organisational and contractual framework as the original Cloud Services.

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 Google.

Google declared services have been externally certified and audited, e.g., Google holds current ISO/IEC 27001:2013 certificates. The declaration of adherence referred to the respective ISO/IEC 27001:2013 certifications 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[16], 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 Google which outlined how all the requirements of the Code were met. 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.E, 5.1.F, 5.2.A, 5.2.C, 5.3.B, 5.4.B, 5.4.D, 5.4.E, 5.4.F, 5.5.B, 5.5.D, 5.7.A, 5.8.A, 5.9.B, 5.10.A, 5.10.B, 5.11.B, 5.12.D, 5.12.E, 5.12.F, 5.14.F, 6.1.A and 6.1.B.

4.3.2 Findings by the Monitoring Body

The Monitoring Body would like to highlight that Google consistently prepared the declaration of adherence well and thoroughly, during the process of verification. Feedback from the previous declara-

[15] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/
[16] You can access the Verification Report(s) of previous year(s) via the following link(s): Verification Report 2021, Verification Report 2020.

tion of adherence in terms of follow-up questions was integrated to the Controls Catalogue Questionnaire. Google's responses were detailed and never created the impression of intentional non-transparency. Requests for clarification, additional and supporting information, as well as relevant samples were promptly dealt with.

Although the renewal has been triggered by Google in due time, the process was not completed within the validation period, as transparently communicated by the Public Register. Delays resulted from administrative factors.

Related to the Monitoring Body's requests (see section 4.1), Google provided the necessary information and confirmations. The assessment did not unfold any aspects that might indicate differently.

The Monitoring Body assessed Google's procedures and alternative options provided to the Customers related to the possibility to reject replacements of or additions of subprocessors. Google provided the Monitoring Body with a paraphrasing of its implemented measures. The Monitoring Body requested information, e.g., by which means the information will be shared to Customers as well as statistical information on how often the process to notify Customers was triggered in 2022. The information provided convincingly indicated compliance with the requirements of the Code.

Another area of focus was around transfer of Customer Personal Data to third countries. Google indicated safeguarding such transfers, at a minimum, by Standard Contractual Clauses (SCCs). In case other safeguards are adopted – in addition to the SCCs – their validity and adequate implementation shall be monitored as applicable. In addition to this, Google indicated having fully transitioned to the new SCCs, alongside supporting documentation.

In the context of determining, whether a representative pursuant Art. 27 GDPR must be appointed or whether European establishments are upheld, Google provided the Monitoring Body with a link of Google Contracting Entities. The contracting entity will be determined per Customer's billing address.

In addition to this, the assessment focused on the possibility for Customers to request additional evidence of compliance and that related communication channels are adequately communicated. Google provided the Monitoring Body with an explanation on the relevant communication channels through which Customers can request additional evidence of compliance, beyond respectively without necessarily exercising their audit rights, which convincingly indicated compliance with the Code.

An overview of the key elements of the procedure to respond to requests by supervisory authorities was provided by Google, as well as explanations on documented procedures in relation to addressing data subjects' requests, convincingly indicating that related procedures comply with the Code.

The Monitoring Body assessed the implementation of a training programme as required by the Code. The training programme, as identified by Google included mandatory internal training during the onboarding procedure which is dependent on the role of the relevant personnel. Training shall be triggered by email and there are escalation procedures for not taking mandatory training within the timeline set internally. In addition to this, Google confirmed that although, not mandatory, certifications are regularly taken by Google personnel to enhance knowledge in data protection and security aspects of their role.

Google maintains an up-to-date and accurate ROPAs of activities carried out on behalf of Customers. In addition to this, the relevant communication channels for Customers providing the relevant information in relation to the completion and relevancy of the ROPA were confirmed by Google.

Current and applicable ISO certifications, covering all Cloud Services and valid for the duration of the declaration of adherence, were provided. The Monitoring Body relied on such external report and certifications, to the extent they meet the criteria set out in the Code, which is indicated where such international audit or certification is already being mapped within the Control's Catalogue.

5 Conclusion

The information provided by Google were consistent. Where necessary, Google 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[17] alongside this report.

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

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

6 Validity

This verification is valid for one year. The full report consists of 13 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[18].

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

Verification-ID: 2020LVL02SCOPE015

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