Verification of Declaration of Adherence

Declaring Company: Google LLC

Verification-ID	2020LVL02SCOPE015
Date of Approval	December 2024
Valid until	December 2025

Table of Contents

SCOPE Europe SRL
Rue de la Science 37
1040 BRUSSELS
https://scope-europe.eu
info@scope-europe.eu

Managing Director
Gabriela Mercuri

Company Register: 0671.468.741
VAT: BE 0671.468.741

ING Belgium
IBAN BE14 3631 6553 4883
SWIFT / BIC: BBRUBEBB

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 Google Workspace[6]

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.[7]

- Admin Console
- Assignments
- Classroom
- Cloud Identity
- Cloud Search
- Gemini for Google Workspace
- Gemini
- Gmail
- Google Calendar
- Google Chat
- Google Contacts
- Google Docs
- Google Drive
- Google Forms
- Google Groups
- Google Jamboard
- Google Keep
- Google Meet
- Google Sheets
- Google Sites

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://workspace.google.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.

- Google Slides
- Google Tasks
- Google Vault
- Google Vids
- Google Voice
- Google Workspace Migrate
- Mobile Device Management
- Read Along

2.2 Google Cloud Platform[8]

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.[9]

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- AI Platform Training and Prediction
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Registry
- Assured Workloads
- AutoML Natural Language
- AutoML Tables
- AutoML Translation
- AutoML Video
- AutoML Vision
- Backup and DR Service
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium (formerly BeyondCorp Enterprise)
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)

[8] https://cloud.google.com/
[9] **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.

- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- 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 NGFW (formerly Cloud Firewall)
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- 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
- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI (formerly Contact Center AI (CCAI))
- Conversational Insights (formerly Contact Center AI Insights)
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Discovery Solutions
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Gemini for Google Cloud
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Contact Center as a Service (CCaaS) (formerly CCAI Platform)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud NetApp Volumes
- Google Cloud VMware Engine (GCVE)
- Google Earth Engine

- Google Kubernetes Engine
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Microsoft Active Directory (AD)
- Media CDN
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- Persistent Disk
- Pub/Sub
- reCAPTCHA Enterprise
- Recommendations AI
- Recommender
- Resource Manager API
- Retail Search
- Risk Manager
- Secret Manager
- Secure Source Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text
- Speech-to-Text On-Prem
- Storage Transfer Service
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Vertex AI Conversation
- Vertex AI Data Labeling
- Vertex AI Platform
- Vertex AI Search
- Video Intelligence API
- Virtual Private Cloud
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

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[10].

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[11].

The Code has been officially approved in May 2021[12]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[13]. 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.[14]

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

---

10 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
11 https://scope-europe.eu
12 https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
13 https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
14 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[15] and referring to the Public Register of the EU Cloud CoC[16] 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.

As this declaration is a renewal[17], the Monitoring Body requested from Google a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Google a comparison of the declared Cloud

---

[15] https://eucoc.cloud/en/public-register/levels-of-compliance/
[16] https://eucoc.cloud/en/public-register/
[17] You can access the Verification Report of previous year via the following link: Google - Verification Report – (2023)

Services of last year and this year as well as to explicitly indicate any Cloud Services that are no longer included in the 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, organisational and contractual framework as the original Cloud Services.

Google 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. This information was completed by the confirmations requested by the Monitoring Body as well as a detailed comparison of the declared Cloud Services between last year and this year verification highlighting the changes and the reasons for them.

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[18], the Monitoring Body analysed the responses and information provided by Google.

Google's declared services have been externally certified and audited. Google holds ISO 27001, 27017, 27018 and 27701 certificates, which are 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 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 verified the certification and references. Further in-depth checks were not performed, as provided third-party certifications adequately indicated compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

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

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

review were: 5.1.B, 5.1.E, 5.1.G, 5.2.D-E, 5.3.C-D, 5.3.F, 5.5.F, 5.7.C-D, 5.11.A, 5.11.C, 5.13.A, 5.14.C-E, 6.1.D, 6.2.A-Q, 6.2.I, 6.2.P, and 6.2.I.

4.3.2 Findings by the Monitoring Body

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

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

Google has indicated that a Cloud Service Agreement (CSA) is in place with Customers defining the processing activities in relation to Customer Personal Data engaged by the CSP and any subprocessors, and the scope of Customer's instructions for the processing of such Data. Additionally, Google indicated that its adherence to the Code is adequately communicated to its personnel and that its personnel is aware of the consequences of adherence. The Monitoring Body confirmed Google's public communication of its adherence to the Code.

The assessment involved the subprocessor management process. Based on the information provided by Google, a review process is in place to ensure that Google only engages subprocessors that can provide sufficient guarantees of compliance with GDPR. Moreover, Google has implemented procedures that ensure a flow down data protection obligations and appropriate technical and organisational measures no less protective than provided by Google to the Customer. Additionally, Google has established a mechanism whereby the Customer is notified of any changes concerning an addition or a replacement of a subprocessor engaged by Google.

Another area of the assessment has been the Data Protection Impact Assessment (DPIA). Google indicated that it assists the Customer with its DPIA by providing the Customer with relevant information. In addition to this, Google maintains documented procedures to ensure that information provided to a Customer for their DPIA does not create a security risk for Google.

Furthermore, Google has implemented policies and procedures to provide Customers with assistance to respond to requests by supervisory authorities, including notification of Customers when it receives a request from the supervisory authority pertaining to Customer Personal Data, as provided by the Code.

Data breach notification and reporting obligations have been in the scope of the assessment. In this vein, Google confirmed that policies and procedures are implemented to identify and handle data breaches without undue delay, if any such breach should happen.

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 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 Google to support the compliance of its service, the Monitoring Body grants Google with a Second Level of Compliance.

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[20].

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

Verification-ID: 2020LVL02SCOPE015

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